INDIAN STATISTICAL INSTITUTE

Periodical Examination

M. Tech (CS) - II Year (Semester - I)

Advanced Algorithms for Graph and Combinatorial Optimization Problems

Date: 4.9.2017 Maximum Marks: 60 Duration: 3 Hours

Note : You may answer any part of any question, but maximum you can score is 60.

1. In a *simple network* each node has either indegree 1 or outdegree 1.

   Consider a simple *unit capacity* network. Show that the distance ℓ between the source s and the sink t cannot exceed $\frac{|V|}{f}$, where V is the set of vertices in the network and f is the value of the maximum flow. [10]

2. Design a recursive linear time algorithm for computing a matching of maximum cardinality of a tree $T = (V, E)$. Justify the correctness and time complexity of your algorithm. [10]

3. In the context of designing an algorithm for computing the maximum matching for a non-bipartite graph, the following result is important: *If at some stage of augmenting the matching, there is no augmenting path from a node u, then there will never be an augmenting path from u in the subsequent stages.* Prove this statement, and state why it is important. [10]

4. Show that, for an undirected and unweighted graph G, the MAXCUT problem is NP-hard.

   Propose an efficient polynomial time factor 2 approximation algorithm for the MAXCUT problem of the graph G. (You are allowed to propose either a deterministic or a randomized algorithm for this purpose. In the formar case, you need to justify the approximation factor and time complexity, and in the later case you need to justify the expected cut size and the time complexity.)

   [10+10 = 20]

5. Let $G = (V, E)$ be an unweighted undirected planar graph, $n = |V|$.

   You have a blackbox that, if G is connected, can compute a separator C of the vertices V whose removal creates two disjoint and disconnected subsets A and B of V $(A \cup B \cup C = V)$ such that $\max(|A|, |B|) \leq \frac{2}{3}n$ and $|C| \leq L(\ell) + L(\ell') + 2(\ell' - \ell - 1)$, where

   - $L(i)$ = number of vertices which are at distance i from a fixed vertex $v \in V$, $L(0) = 1$,
   - r = maximum distance of a vertex from v.
   - ℓ and ℓ' be two levels $(\ell \leq \ell')$ such that the total number of vertices from level 0 to $L(\ell - 1)$ is not exceeding $\frac{2}{3}n$, and total number of vertices from level $L(\ell' + 1)$ to r is not exceeding $\frac{2}{3}n$.

   Use this blackbox or otherwise find a separator C^* of the vertices of V whose removal creates two disjoint and disconnected subsets A and B of V $(A \cup B \cup C = V)$ such that $\max(|A|, |B|) \leq \frac{2}{3}n$ and $|C| = O(\sqrt{n})$.

   You must consider both the cases where (i) G is connected, and (ii) G is not connected.

   [10+10=20]

6. Consider the following algorithm for computing the *maximum independent set* (MIS) of a planar graph $G = (V, E)$.

   - Choose an appropriate vertex $v \in V$,
   - include v in the independent set S,
   - delete v and all its neighbors from V, and
   - repeat the process on the graph G' obtained in the earlier step unless $V = \emptyset$.

   For what choice of v in each step, we can get a constant factor approximation algorithm for the MIS problem of the planar graph? State the time complexity of this algorithm and justify. [4+6=10]

Indian Statistical Institute

M.Tech (CS) II

Information and Coding Theory

Mid Semester Examination

Maximum Marks: 70

Date: September 4, 2017.
Time 2.5 hours

The question paper contains 7 questions. Total marks is 70. Maximum you can score is 60. Unless otherwise mentioned, all notations are the same as presented in class.

1. Let X, Y and Z be joint random variables. Prove the following inequalities and find conditions for equality.

   (a) $H(X,Y|Z) \geq H(X|Z)$.

   (b) $I(X,Y;Z) \geq I(X;Z)$.

   (c) $H(X,Y,Z) - H(X,Y) \leq H(X,Z) - H(X)$.

   (d) $I(X;Z|Y) \geq I(Z;Y|X) - I(Z;Y) + I(X;Z)$.

   (3+3+3+3 = 12)

2. Show that the entropy of the probability distribution, $(p_1,\ldots,p_i,\ldots,p_j,\ldots,p_m)$, is less than the entropy of the distribution $(p_1,\ldots,\frac{p_i+p_j}{2},\ldots,\frac{p_j+p_i}{2},\ldots,p_m)$. (5)

3. Let $X_1, X_2, \ldots$ be independent, identically distributed random variables drawn according to the probability mass function $p(x), x \in \{1,2,\ldots,m\}$. Thus, $p(x_1,x_2,\ldots,x_n) = \Pi_{i=1}^{n} p(x_i)$. We know that $-\frac{1}{n}\log p(X_1,X_2,\ldots,X_n) \to H(X)$ in probability.

   Let $q(x_1,x_2,\ldots,x_n) = \Pi_{i=1}^{n} q(x_i)$, where q is another probability mass function on $\{1,2,\ldots,m\}$.

   (a) Evaluate $lim - \frac{1}{n}\log q(X_1,X_2,\ldots,X_n)$, where $X_1,X_2,\ldots$ are i.i.d. $\sim p(x)$.

   (b) Evaluate the limit of the log likelihood ratio $\frac{1}{n}\log\frac{q(X_1,\ldots,X_n)}{p(X_1,\ldots,X_n)}$ when $X_1,X_2,\ldots$ are i.i.d. $\sim p(x)$. (6 + 6 = 12)

4. Consider the following method for generating a code for a random variable X which takes on m values $\{1,2,\ldots,m\}$ with probabilities $p_1,p_2,\cdots,p_m$. Assume that the probabilities are ordered so that $p_1 \geq p_2 \geq \cdots \geq p_m$. Define

   $$F_i = \sum_{k=1}^{i-1} p_k.$$

   Then the codeword for i is the number $F_i \in [0,1]$ rounded off to l_i bits, where $l_i = \lceil \log\frac{1}{p_i} \rceil$.

   (a) Show that the code constructed by this process is prefix-free and the average length satisfies

   $$H(X) \leq L < H(X) + 1.$$

   (b) Construct the code for the probability distribution $(0.5, 0.25, 0.125, 0.125)$.

   (5 + 4 + 3 = 12)

5. Let $X_1, X_2, \ldots, X_{n-1}$ be i.i.d. random variables taking values in $\{0,1\}$ with $Pr\{X_i = 1\} = 1/2$. Let $X_n = 1$ if $\sum_{i=1}^{n-1} X_i$ is odd and $X_n = 0$ otherwise. Let $n \geq 3$.

   (a) Show that X_i and X_j are independent, for $i \neq j$, $i, j \in \{1, 2, \ldots, n\}$.

   (b) Find $H(X_i, X_j)$, for $i = j$.

   (c) Find $H(X_1, X_2, \ldots, X_n)$. Is this equal to $nH(X_1)$?

   $(6 + 2 + 4 = 12)$

6. Consider the discrete memoryless channel $Y = X + Z(\text{mod}\,11)$, where

$$Z = \begin{pmatrix} 1, & 2, & 3 \\ 1/3, & 1/3, & 1/3 \end{pmatrix},$$

   and $X \in \{0, 1, \ldots, 10\}$. Assume that Z is independent of X.

   (a) Calculate the channel capacity.

   (b) For what distribution of X is this capacity achieved? $(4 + 1{=}5)$

7. Find the entropy rate of the Markov chain associated with a random walk of a (i) Bishop (ii) Rook on a 8×8 chessboard. (6+6=12)

Natural Language Processing
Question for Mid Semestral Examination M. Tech CS 2nd Year, 2017-2018
Indian Statistical Institute, Kolkata
Time Limit: 3 hrs
Total Marks: 75, Maximum Score: 60
NOTE:
Open book test. Any material including mobile, the internet access is permissible.

---

1. The vocabulary set $\mathcal{V}$ of a language consists of m distinct words ($m > 1$). There are two special words $START$ and $STOP$. To build a n-gram language model with the above vocabulary and the two special words, every possible n-gram must satisfy the following properties:

   For any n-gram $< w_1, w_2, \ldots, w_n >$,

   (a) $w_n \in STOP \cup \mathcal{V}$

   (b) for $i = 2$ to $n-1$, w_i can be $START$ if and only if for $j = 1$ to $i-1$, $w_j = START$

   (c) $w_1 \in START \cup \mathcal{V}$

   Calculate the total number of distinct and possible n-grams for the above language model. (**10 Marks**)

2. S → S Prep S
   S → S Verb S
   S → W
   W → Uncle
   W → Akash
   W → Jatin
   Prep → of
   Verb → scolds

   Consider the above CFG and answer the following questions.

   (a) Why is the Grammar ambiguous?

   (b) Show two different parses of the sting
   Uncle of Akash scolds Jatin.

   (c) Compute the probabilities of parse trees if the rule probabilities are 0.4, 0.4, 0.2, 0.3, 0.3, 0.3, 1.0, 1.0, respectively.

   (d) Why are the probabilities different or why are the same?

   Marks: 2 + 3 + 3 + 2 = 10

3. A new model for statistical machine translation is defined as follows:
$p(f,a|e,m) = \prod_{i=1}^{m} t(f_i|e_{a_i}) \times q(a_i|a_{i-1},l,m)$

Here f is a French sentence $f_1,\ldots,f_m$. a is the sequence of alignment variables $a_1,\ldots,a_m$ and e is an English sentence $e_1,\ldots,e_l$. t is the translation parameter and q is the alignment parameter. We assume that a_0 is defined to be 0. Note that in contrast to the IBM Model 2, the alignment parameters are modified to be conditioned upon the previous alignment variable. That is, alignment of i^{th} French word depends on the alignment of $(i-1)^{th}$ French word.

Given the training data (f^k, e^k) for $k = 1$ to n where lengths of f^k and e^k are m_k and l_k respectively.

(a) Write down the model's parameter estimation algorithm for fully observed data. **(10 Marks)**

(b) Write down the model's parameter estimation algorithm for partially observed data. **(15 Marks)**
[Hint: At first define the $count()$ variables carefully.]

4. Consider the bi-gram HMM given below. There are two tags N and V which can emit words. Two special tags 'start' and 'stop' cannot emit words. The vocabulary set = {'I', 'You', 'He'}. The word emission probabilities are given below.

$p('I'|N) = 0.2$, $p('You'|N) = 0.4$, $p('He'|N) = 0.4$
$p('I'|V) = 0.5$, $p('You'|V) = 0.4$, $p('He'|V) = 0.1$

The observation sequence is 'He I He'.

(a) Find the most probable tag sequence for the observation using Viterbi algorithm. **(10 Marks)**

(b) Assuming the values of all the parameters of the above HMM as initial values and the given observation, estimate $p(N|start)$ and $p(V|start)$ for the next iteration. **(10 Marks)**
Also estimate $p('I'|N)$ and $p('I'|V)$ for the next iteration. **(10 Marks)**

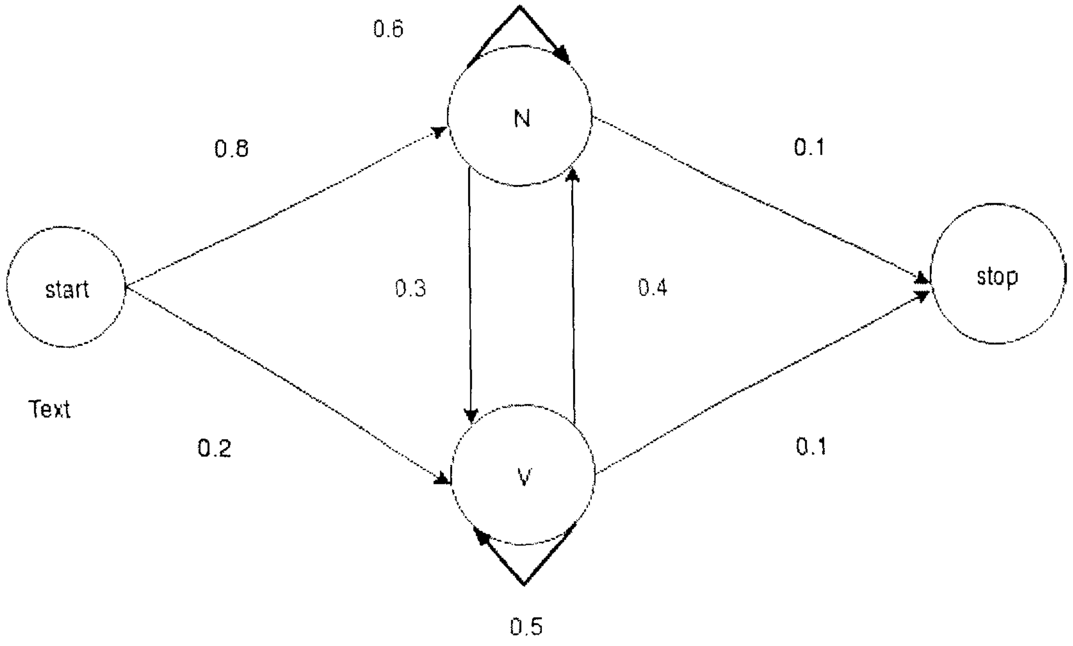


Figure 1: Automaton for the HMM.

Indian Statistical Institute

Semister-I 2016-2017

M.Tech.(CS) - Second Year

Mid-term Examination (September 5, 2017)

Subject: **Patter Recognition and Image Processing**

Total marks: 80 Duration: 2 Hours

1.

a) Imagine that you are given the following set of training examples. Each feature can take one of three nominal values: a, b, or c.

F1	F2	F3	Class Label
a	c	a	+
c	a	c	+
a	a	c	–
b	c	a	–
c	c	b	–

Table 1: A sample dataset. Here, F_i's are the features.

i. How would a Naive Bayes" classifier classify the following test example? Be sure to show your work.

Test example: F1 = a, F2 = c, F3 = b (6 Marks)

ii. Describe how a 3-nearest neighbor algorithm would classify the test example given above. (4 Marks)

b) Discuss: (i) Ensemble of Classifiers, (ii) Support Vector Machine (SVM) (5 Marks)

c) What is a confusion matrix for binary and multi-class classification problems? Discuss few evaluation measures defined using this matrix. (5 Marks)

2. a) First consider the data plotted in Figure 1, which consist of two rows of equally spaced points. If k-means clustering (k = 2) is initialized with the two points whose coordinates are (9, 3) and (11, 3), indicate the final clusters obtained (after the algorithm converges) on the data of Figure 1. (6 Marks)

P.T.O

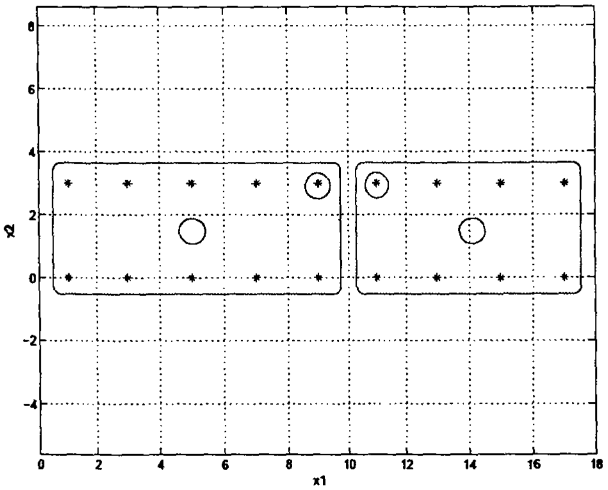


Figure 1: A data set for clustering.

b) Cluster these five points using: (i) single linkage, (ii) complete linkage, and (iii) average linkage. Draw the dendrograms to depict the clustering you obtain. (8 Marks)

	P_1	P_2	P_3	P_4	P_5
P_1	1	0.92	0.35	0.22	0.21
P_2	0.92	1	0.61	0.44	0.16
P_3	0.35	0.61	1	0.37	0.1
P_4	0.22	0.44	0.37	1	0.33
P_5	0.21	0.16	0.1	0.33	1

Table 2: Similarities between five patterns (P).

c) Discuss:

i. DBScan. Why is it important to consider density when clustering a dataset? Illustrate your argument(s) with examples.

ii. K-Medoids. Discuss an effective way to choose appropriate initial centroids. Illustrate situations in which one way would be more appropriate than the others. (6 Marks)

3. a) Define the covariance matrix and discuss its properties. (4 Marks)

b) What is cross validation? (2 Marks)

c) What is the difference between feature extraction and selection? (5 Marks)

d) Apply the Principal Component Analysis (PCA) and compute the principal components of the following two dimensional data. (9 Marks)

	P_1	P_2	P_3	P_4
F_1	6	-3	-2	7
F_2	-4	5	6	-3

Table 3: Two dimensional data for PCA.

INDIAN STATISTICAL INSTITUTE

Mid-Semestral Examination:(2017-2018)

M.TECH (CS) II YEAR

Subject Name: Quantum Information Processing and Quantum Computation

Maximum Marks: 30 Duration: 2 hours Date: 06/09/2017

Answer any three of the following four questions

1. a) Let the state of a spin 1/2 particle is $|0\rangle$ which is eigen state of σ_z. Show that the results of any spin measurement along any direction in x-y plane is completely random.

b) There is a cloning machine which clones two orthogonal states $|\psi_1>$ and $|\psi_2>$. Then show that by this machine one can not clone any state which is superposition of these two states.

c) Consider a Swap operator U_s which acts in the following way:

$$U_s|\psi\rangle \otimes |\phi\rangle = |\phi\rangle \otimes |\psi\rangle$$

for all possible states $|\psi\rangle$, $|\phi\rangle$. Realize a two-qubit swap gate using the CNOT gate.

[3+3+4]

2. a) Let Alice and Bob share the following state;

$$|\psi>_{AB}=\frac{1}{\sqrt{5}}(|0>_A|0>_B+\frac{2}{\sqrt{5}}|1>_A|1>_B)$$

where $|0\rangle$ and $|1\rangle$ are eigen states of σ_z.
(i) Show that the state can not be written as $|\phi>\otimes|\chi>$.
(ii) Show that the state can be transformed to a maximally entangled state by local operations and classical communications with probability $\frac{1}{5}$.

b) Consider the following state which is eigenstate of $\sigma_z \otimes \sigma_z$

$$|\phi>_{AB}= c_0|0>_A\ |0>_B + c_1|1>_A\ |1>_B$$

Under what condition the state will also be eigen state of $\sigma_x \otimes \sigma_x$.

[(2 + 5) + 3]

3. i) Consider a two qubits pure state $|\psi\rangle_{12}$ and four unitary operators $\{U_i, i = 1, 2, 3, 4\}$ acting on the first particle. What is the necessary condition so that the four states $\{U_i \otimes I|\psi\rangle_{12}, i = 1, 2, 3, 4\}$ form an orthogonal set?

ii) Find a two qubits state $|\psi\rangle_{12}$ and unitary operators for which $\{U_i \otimes I|\psi\rangle_{12}, i = 1, 2, 3, 4\}$ form an orthogonal set.

iii) Discuss how quantum super dense coding can be realized using the by using a maximally entangled state.

[2 + 3 + 5]

4. a) Consider following two states $|0\rangle$ and $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, where $|0>$ and $|1>$ are two orthogonal vectors. Show that these two states can not be reliably cloned.

b) Aice, Bob and Charlie are in three different labs. Charlie and Alice shares a two-qubit state;

$$|\phi>_{AB}= c_0|0>_C\ |0>_A + c_1|1>_C\ |1>_A$$

and Alice and Bob share another two-qubit state;

$$|\phi^+>_{AB}= \frac{1}{\sqrt{2}}|0>_A\ |0>_B + \frac{1}{\sqrt{2}}|1>_A\ |1>_B$$

Show that using quantum teleportation the entanglement between Charlie and Alice can be transferred to Charlie and Bob.

$2 + 8$

Indian Statistical Institute

Mid-Semester Examination : 2017 – 2018

Master of Technology in Computer Science, Semester III

Functional Brain Signal Processing: EEG & fMRI

Date: 6 September 2017 Maximum Marks: 50 Duration: 2 hours

Attempt all the questions. Credit will be given for precise and brief answers.

1. Consider the Butterworth filter with the amplitude response $|H(\omega)| = \dfrac{1}{\left\{1+\left(\dfrac{\omega}{\omega_c}\right)^{2N}\right\}^{\frac{1}{2}}}$, where $H(\omega)$ is the impulse response system function, ω is frequency, ω_c is cutoff frequency and N (positive integer) is order of the filter. Explain with reason if it is a high-pass or low-pass filter. If it is a high-pass filter, describe how to make it a low-pass filter and vice-versa. For $N=1$ show the amplitude response plot taking values of your choice. 3 + 3 + 6 = 12
2. Write short notes on any four important uses of EEG according to your choice. 4 x 3 = 12
3. a) For the independent component analysis (ICA) algorithm to be applicable why the data set must not be distributed normally? How does it give a measure to implement the ICA algorithm? An outline indicating the steps will have to be given. Precise mathematical expressions are not essential. 3 + 4 = 7

   b) Why logistic regression algorithm converges exponentially fast during the training? 3

   c) Principal component analysis (PCA) will be most effective when the components of the data are oriented orthogonally – explain (no mathematical proof is required). 4
4. Write short notes on alpha, beta and gamma bands of EEG, and event related potential. 4 x 3 = 12

INDIAN STATISTICAL INSTITUTE

Mid-Semester Examination: 2016-2017

M. Tech. (CS) II year

Data Mining and Knowledge Discovery

Date: 06.09.2016 **Maximum Marks: 50** **Duration: 2 hours**

[Answer as much as you can]

1. (i) Outline the basic steps of knowledge discovery in databases.
   (ii)What is the difference between classification and prediction?
   (iii) How do we evaluate classification methods?
   (iv) Elaborate on the tree induction strategy.
   (v) What is cross validation? [4+3+3+5+4=19]

2. (i) What are the different ways of performing split, in the context of decision trees?
   (ii) Outline the measures of evaluating node impurity.
   (iii) Indicate the stopping criteria in decision tree classifiers.
   (iv) How can we compare two or more classifiers?
   (v) What is an AVC set? [4+5+4+4+4=21]

3. One major challenge when learning prediction and classification models is to avoid overfitting.
   (i)What is overfitting? What factors contribute to overfitting?
   (ii)What is generalization error? What is the challenge in determining generalization error?
   (iii)Briefly describe one approach to determine generalization error. [5+5+3=13]

4. (i) Briefly explain the difference between (batch) gradient descent and stochastic gradient descent. Give an example of when you might prefer one over the other.
   (ii) What is the purpose of momentum? What is the difference between standard Momentum and Nesterov Momentum?
   (iii) In mini-batch gradient descent which one is more important – "number of mini-batch updates" or "visiting all of the training data" – and why? [4+4+5=13]

5. (i) Compare and contrast (providing specific differences, advantages and disadvantages) between the following optimization algorithms: Adagrad, RMSprop, Adadelta.
   (ii)Discuss different feature rescaling techniques in brief. [6+4=10]

INDIAN STATISTICAL INSTITUTE

Mid Semestral Examination:(2016-2017)

MTech C.S. 2nd Year

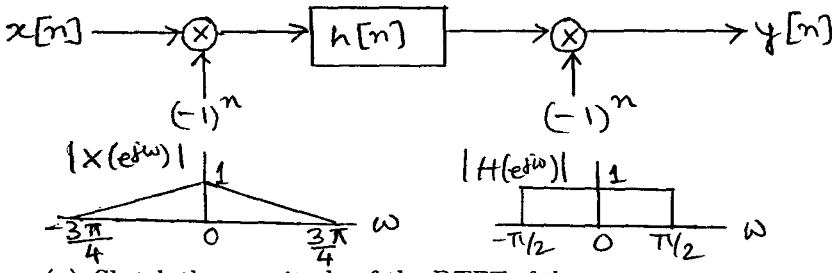
Digital Signal Processing

Date: 7.9.2017 Maximum Marks: 60 Duration: 2 hours

Note: The examination is open book, open notes. The marks add up to 70. The maximum you can score is 60. Use of calculators is permitted.

1. Determine the output of an LTI system with impulse response $h[n] = (-0.2)^n u[n]$ and input $x[n] = (0.3)^n u[n]$. [5]

2. For the system shown below and input signal and the LTI system having Discrete Time Fourier Transforms (DTFT) magnitudes as indicated :



   (a) Sketch the magnitude of the DTFT of the output.

   (b) Sketch the magnitude response of $H(z)H(-z^2)$.

[10+8]

3. The impulse response of an LTI system is:

$$h[n] = 3\delta[n] - 5\delta[n-1] + \delta[n-2] + a\delta[n-3] + b\delta[n-4]$$

where $\delta[n]$ is the unit impulse sequence.

   (a) Is the system causal? Justify your answer.

   (b) Determine a and b such that the impulse response is even.

   (c) For the values of a and b that you have determined, determine the phase of the system. Does the system have linear phase?

[5+5+(5+3)]

4. A causal LTI system has the impulse response

$$h[n] = A\delta[n] + B\alpha^n u[n]$$

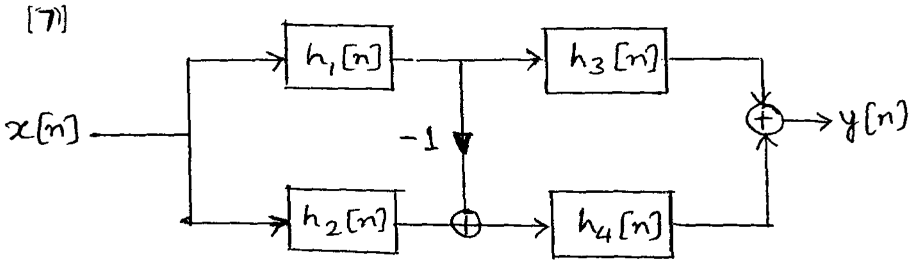
where $u[n]$ stands for the unit step sequence and $|\alpha| < 1$. Let the causal inverse system be of the form

$$g[n] = C\delta[n] + Du[n]$$

Determine C and D. [10]

5. For the system shown below, determine the overall impulse response:

[7]



6. (a) Determine the inverse z-transform of

$$X(z) = \log(1 - \frac{1}{\alpha}z^{-1}), \qquad |z| > |1/\alpha|$$

(b) The system function of an LTI system is given by:

$$H(z) = \frac{z^{-1}(1 + 1.8z^{-1})(1 - 4z^{-1})}{(1 + 0.3z^{-1})(1 - 0.6z^{-1})(1 + 0.5z^{-1})}$$

Determine if the frequency response exists and if the system can be causal. [8 +(3+3)]

Artificial Intelligence

Mid-Semester Examination 2017

Full marks 100

Answer any 5 questions

Duration 3 hours.

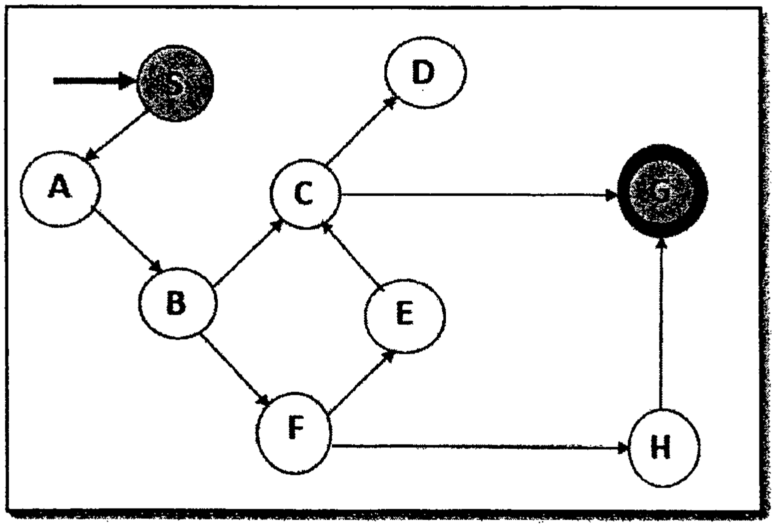
07/9/17

1) Using **DEPTH FIRST SEARCH (DFS)**, traverse the following graph from its start node to its goal node to obtain the shortest path (20)

(i) What data structure is needed to solve the graph using DFS and why?

(ii) Form the tree structure of the given graph and show the direction of reaching the goal node first using DFS.

(iii)Show the entire operations of the data structure used for solving the graph using DFS.



GRAPH : HERE 'S' IS THE START NODE AND 'G' IS THE GOAL NODE

2) Consider the following problem of missionaries and cannibals; (20)
3 missionaries and 3 cannibals are on the left bank of a river. They (all 6 people) must cross the river to reach the right bank. A small boat is available but it can carry only two people at a time. Also, if the cannibals outnumber the missionaries, at any instant, the cannibals eat the missionaries. They must use the boat to cross the river so that all the 3 missionaries can survive.

P.T.O

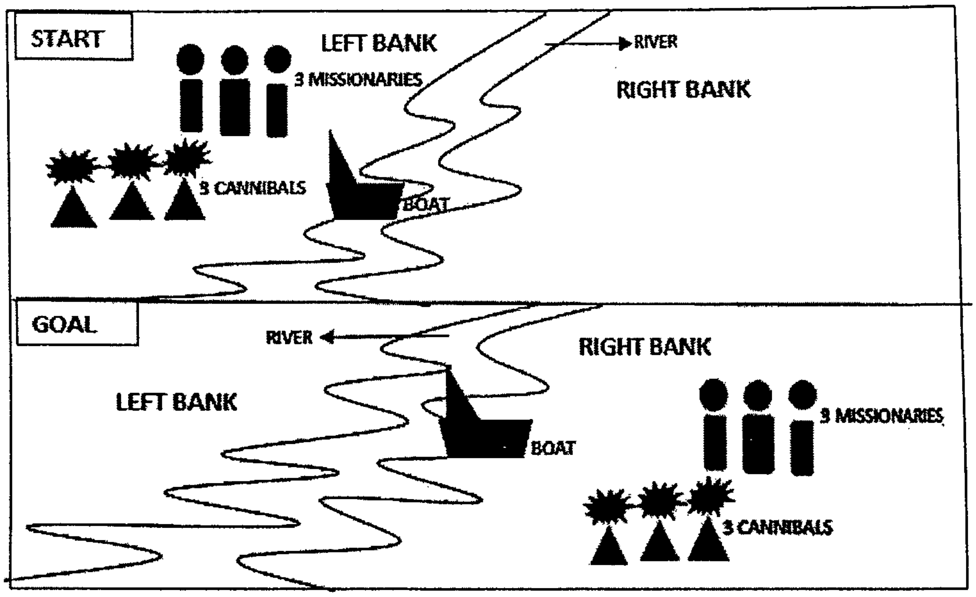
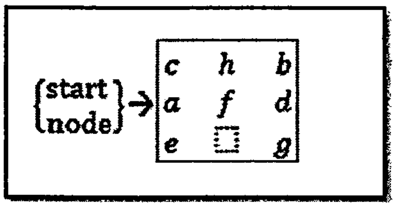


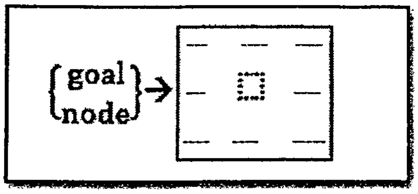
FIGURE: Pictorial representation of missionaries and cannibals problem.
To design the state space graph of the above problem, form the following ***elements:*** (i) form the suitable set of states, (ii) define suitable initial state, (iii) form the goal state depending on the given aim of the problem, (iv) form the suitable set of operators by defining each with the help of equations so that it can meaningfully become the tool for transition from one state to another, eventually reaching the goal state, (v) form the corresponding pre-conditions for the operators. define all the operators in the tabular form and show the preconditions and application of an operator.

3) Solve the following 8-puzzle/ 8-tiles problem using A*- algorithm. Mention the evaluation function of the same problem, show the tabulated solution of the problem using list OPEN and show the graphical representation of the same solution. Also, show the backtracking to the optimal path after reaching the solution. **(20)**



c	*h*	*b*
a	*f*	*d*
e	□	*g*

Bring the empty tile or the square box at the center of the goal node as shown below, irrespective of the positions of the elements a,b,c,d,e,f,g,h



—	—	—
—	□	—
—	—	—

p·T·O

4) Let U = {u} = {1, 2, 3} and V = {v} = {1,2, 3, 4}. The fuzzy conditional statement expressing the dependence between two linguistic variables L and K is: IF (L is "low") THEN (K is "high") where "low" = {1/1, 0.7/2, 0.3/3} and "high" = {0.2/1, 0.5/2, 0.8/3, ¼}. (20)

i) Now define L="medium" in terms of primary fuzzy set defined over the universe U.

ii) Develop a fuzzy relation from the above mentioned IF-THEN rule considering MIN operator as the semantic of fuzzy implication (i.e. fuzzy IF-THEN) operator.

iii) Deduce the fuzzy consequence K under the observation of L="medium".

Note that for such deduction you may use fuzzy compositional rule of inference (You may consider MAX-MIN composition for simplicity of computation)

iv) Derive the defuzzy value of the consequence K under the observation L="medium".

5) Suppose we can perform the following chemical reactions: (20)

i) MgO + H_2 $\rightarrow$ Mg + H_2 O

ii) C + O_2 $\rightarrow$ C O_2

iii) C O_2 + H_2 0 $\rightarrow$ H_2 C O_3.

For this problem we may consider MgO, H_2, O_2 and C as atomic formulas. Then the above chemical reactions i, ii and iii can be represented as i', ii'and iii' .

i') (MgO, Λ H_2) $\rightarrow$ (Mg Λ H_2O)

= ~ (MgO, Λ H_2) V (Mg Λ H_2O)

= (~ MgO V ~ H_2) V (Mg Λ H_2O). Thus we get the following propositional clauses;

F_1 $\underline{\Delta}$ (~MgO V ~ H_2 V Mg) Λ (~MgO V ~ H_2 V H_2O)

ii') (C Λ O_2) $\rightarrow$ C O_2

= ~ (C Λ O_2) V C O_2. Thus we get the following propositional clause;

F_2 $\underline{\Delta}$ ~ C V ~ O_2 V C O_2

iii') (C O_2 Λ H_2O) $\rightarrow$ H_2 C O_3

= ~ (C O_2 Λ H_2O) V H_2 C O_3. Thus we get the following propositional clause;

F_3 $\underline{\Delta}$ ~C O_2 V ~H_2O V H_2 C O_3.

Suppose we have some quantities of MgO, H_2, O_2 and C; that means we have the followings unit clauses.

F_4 $\underline{\Delta}$ Mg O

F_5 $\underline{\Delta}$ H_2

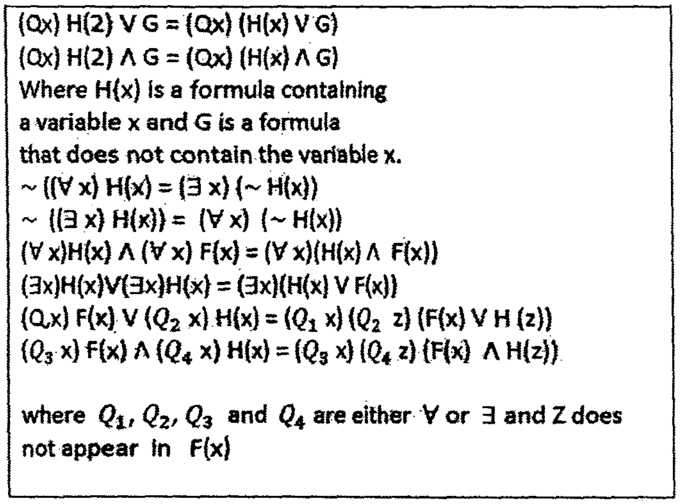
F_6 $\underline{\Delta}$ O_2

p·T·O

F_7 $\underline{\Delta}$ C

By principle of resolution (i.e. proof by contradiction) show that we can make H_2 C O_3.

6) Consider the following equivalent formulas: (20)



$(Qx)\ H(2) \vee G = (Qx)\ (H(x) \vee G)$

$(Qx)\ H(2) \wedge G = (Qx)\ (H(x) \wedge G)$

Where H(x) is a formula containing a variable x and G is a formula that does not contain the variable x.

$\sim ((\forall x)\ H(x) = (\exists x)\ (\sim H(x))$

$\sim ((\exists x)\ H(x)) = (\forall x)\ (\sim H(x))$

$(\forall x)H(x) \wedge (\forall x)\ F(x) = (\forall x)(H(x) \wedge F(x))$

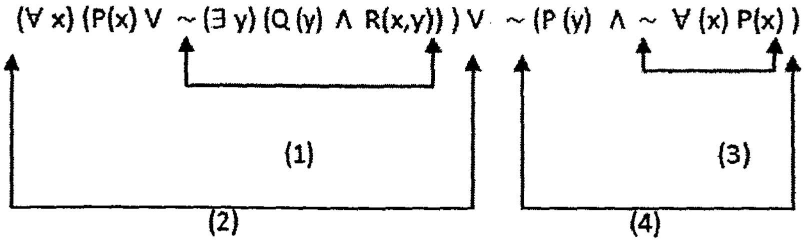
$(\exists x)H(x) \vee (\exists x)H(x) = (\exists x)(H(x) \vee F(x))$

$(Q_1 x)\ F(x) \vee (Q_2\ x)\ H(x) = (Q_1\ x)\ (Q_2\ z)\ (F(x) \vee H\ (z))$

$(Q_3\ x)\ F(x) \wedge (Q_4\ x)\ H(x) = (Q_3\ x)\ (Q_4\ z)\ (F(x)\ \wedge H(z))$

where Q_1, Q_2, Q_3 and Q_4 are either $\forall$ or $\exists$ and Z does not appear in F(x)

Based on the above equivalent formulas and usual equivalent formulas of propositional logic derive the Prenex Normal form of the following expression.



$(\forall x)\ (P(x) \vee \sim (\exists y)\ (Q(y)\ \wedge\ R(x,y)))\ \vee\ \sim (P(y)\ \wedge \sim\ \forall\ (x)\ P(x)\ )$

7) Derive the Skolem standard form of the following expression; (20)

$\sim\ ((\forall x)\ P(x) \rightarrow (\exists y)\ (\forall z)\ Q(y, z))$

Note that at the time of conversion to Skolem standard form you may use all the expressions of the equivalent formulas of propositional logic and predicate logic.

INDIAN STATISTICAL INSTITUTE

Periodical Examination: (2017 – 2018)

M.Tech. (CS) II Year

Parallel Processing: Architectures and Algorithms

Date: 07 /09/2017 Total Marks: 60 Duration: 2 hrs

1. Let us consider two 2×2 matrices A and B. Show the program graph that computes the product matrix C = A × B, and finds the maximum of the four elements of C.
   Consider the operations *multiply* (*), *addition* (+)', and *comparison* (<) as the fine grains.
   For an arbitrary processor, it is given that the addition and comparison operations need 20 CPU cycles each, and the multiply operation takes 100 CPU cycles. The inter-processor communication delay is 200 cycles.

   i) Show the scheduling of the fine grain program using maximum number of processors to utilize the software parallelism existing in the program. Find the *speed-up* and *utilization*.

   ii) If possible, use *grain packing* to improve the *speed-up* and *utilization*, and compare the results with those obtained in (i) and justify.

   [4+4+4=12]

2. a) Show the schematic diagram of a *shared-memory* MIMD computer mentioning its features.

   b) Given a very large unsorted file consisting of *n* distinct entries, it is required to search if a given input *x* is present in the file.
   Write the steps to solve it on an *EREW shared-memory PRAM* with N processors, $N < n$. Find the worst-case time complexity.
   Can you improve the average-case complexity using some flag for early-termination with EREW model? Justify your answer.
   If not, can you choose any other model of *shared-memory* for it?
   What will be the problem, in case the items of the file are not distinct? How can you resolve it using a different memory model?

   [3+(5+3+1+1) = 13]

3. Answer in brief:

   a) Find an expression for the *upper bound* on the number of nodes in a regular graph with node degree *d* and diameter *k*. Why does *Moore graph* exist only for limited values of *d* and *k*?

   b) Prove that if each node of an *NxN* mesh contains one packet to be routed to a unique destination, following the *farthest-first* strategy, routing can be completed in *(2N-2)* steps. Assume that links are bidirectional.

P.T.O

c) Define *a pancake* graph. Show that the upper bound on the diameter of an *n-pancake* graph is (*2n-3*).

d) In a hypercube of degree n, how many distinct shortest paths exist between two nodes u and v, if the shortest distance between the two is of length k, $k \leq n$? Paths are distinct if they differ in at least one intermediate node. Also, find the number of edge-disjoint paths between u and v. Justify your answer.

[5 × 4 = 20]

4. a) Describe the following CUDA programming terminologies with an example:

   i) `__syncthreads( )`

   ii) `Warp Divergence`

   iii) `cudaMemcpy`

b) Given an array A of N integers, write a CUDA kernel function that outputs the maximum element of A.

[(3 × 2) + 9 =15]

INDIAN STATISTICAL INSTITUTE

Periodical Examination

M. Tech (CS) - II

Computational geometry

Date : 08.09.2017 Maximum Marks : 30

Duration : 2 hours.

(Although the paper carries a total marks of 40, the maximum marks you can score is 30)

Question 1: (a) State and prove lower bound for Convex hull of a set P of n points in plane. 5

(b) Describe Chan's algorithm for computing Convex hull of P. 5

Question 2: (a) Let S be a convex polygon of n vertices. Show how to prepare a data structure that uses $O(n)$ storage and time, so that, given any query point q, we can determine, in $O(\log n)$ time, whether q lie inside S. 5

(b) Let S be a set of n points in the plane. Show how to prepare a data structure that uses $O(n)$ storage, so that, given any query line l, we can determine, in $O(\log n)$ time, (a) whether l separates S (i.e., each of the halfplanes bounded by l contains points of S). 5

Question 3: (a) Prove that, in every triangulation of n points in R^2 there exists an independent set of at least $\lfloor \frac{n}{18} \rfloor$ among the vertices of maximum degree 8. Describe an algorithm that finds such a set of vertices in $O(n)$ time. 5

(b) Prove that any triangulated simple polgon (with holes) is 3-colorable? 5

Question 4: Let C_1 and C_2 be two convex polygons, each consisting of n edges. Give linear-time algorithms for the following problems: (a) Determine whether C_1 and C_2 intersect. (b) If they do intersect, compute the intersection $C_1 \cap C_2$ (of their interiors). 5+5

Indian Statistical Institute
Mid-Semestral Examination: 2017
Course Name: M. Tech. in Computer Science II year
Subject Name: Mobile Computing

Date: 09-09-2017 Maximum Marks: 60 Duration: 3 hours

Instructions: You **may** attempt **all** questions which carry a total of **65** marks. However, the maximum marks you can score is only **60**.

1. (a) What is the difference between horizontal handover and vertical handover? [1]

   (b) What is network connection time? [1]

   (c) How network connection time is related to superfluous handover. [1]

   (d) What is unnecessary handover? [1]

   (e) State two main reasons for handover failure. [2]

   (f) Describe an SINR based vertical handover decision algorithm. [3]

   (g) State a limitation of fluid flow mobility model. [1]

   (h) What is difference between soft handover and hard handover? [1]

   (i) Explain with an example the relative signal strength with hysteresis and threshold based hard handover strategy. [3]

   (j) What is Jain's fairness index? [1]

2. (a) Compare the always-update and never-update location management schemes in terms of paging cost and update cost. Which scheme performs better for users with a low mobility rate or high call arrival rate? [3+1=4]

   (b) Briefly describe the time, movement and distance based dynamic location update schemes. [6]

   (c) Briefly describe the process of terminal paging to determine the location of a particular mobile terminal. [3]

   (d) What is blanket polling? [2]

3. (a) State the channel assignment problem (CAP) in cellular network in terms of a generalized vertex coloring problem. [3]

   (b) Briefly describe the method of constructing coalesced CAP from the original CAP. [8]

   (c) Show that if solution of the coalesced CAP produces no call blocking, the solution of the original CAP obtained from the solution of the coalesced CAP is `conflict-free`. [3]

   (d) Explain with an example the forced assignment with rearrangement operation used in perturbation-minimizing frequency assignment problem. [3]

4. (a) Define non-overlapping and partially overlapping channels in WLAN. [2]

   (b) Describe how the interference between both non-overlapping and partially overlapping channels can be modeled using a weighted conflict graph? [5]

   (c) Describe a greedy algorithm based on weighted conflict graph for solving the minimum interference channel assignment problem in WLAN. [8]

   (d) Compare the relative advantages and disadvantages of random polling access and proportional fair access methods in WLAN. [3]

INDIAN STATISTICAL INSTITUTE

Mid Semestral Examination

M. Tech (CS) - II Year, 2017-2018 (Semester - III)

Optimization Techniques

Date : 11 / 09 / 2017 Maximum Marks : 90 Duration : 3.0 Hours

---

Note: The question paper is of 100 marks. Answer as much as you can, but the maximum you can score is 90.

Vectors would be written in small letters with boldface, e.g. b; matrices would be written in capital letters, e.g., A. Transpose of A would be denoted by A^T and transpose of b would be denoted by $\mathbf{b}^T$. Whenever we say that, $\mathcal{P}$ is a linear program, we mean $\mathcal{P}$ is of the form

$$\begin{aligned} \text{Maximize} \quad & \mathbf{c}^T\mathbf{x} \\ \text{subject to} \quad & A\mathbf{x} \leq \mathbf{b} \\ & \mathbf{x} \geq \mathbf{0} \end{aligned}$$

(Q1) The *chromatic number* of a graph $G = (V, E)$ is the minimum number of colors that can be assigned to each vertex of V such that no two vertices in V sharing an edge has the same color. Write a mathematical program to find the chromatic number of a graph. Explain with suitable justifications your deduced mathematical program. [5+5=10]

(Q2) In the *set cover* problem, we have an universe $\mathcal{U} = \{u_1, \dots, u_n\}$ of n elements. Let $\mathcal{S} = \{S_1, \dots, S_m\}$ be a set of m sets, where each set $S_i \subseteq \mathcal{U}$. Each set S_i has a weight $w_i \geq 0$. The problem in *set cover* is to find a minimum weight collection of subsets of $\mathcal{S}$ that covers all elements of $\mathcal{U}$.

(a) Write an integer linear program (ILP) for the *set cover problem* using decision variables x_i to indicate whether the set S_i is included in the solution or not.

(b) Relax the above ILP and round the optimal solution of the linear program as follows: given the optimal solution $\mathbf{x}^*$ of the linear program, we include the subset S_i in our solution if and only if $x_i^* > \frac{1}{f}$, where f is the maximum number of sets in which any element appears and x_i^* is the i-th component of $\mathbf{x}$.

For this rounding scheme, show that the set generated is a set cover and is an f-factor approximation algorithm.

[5+10=15]

(Q3) Describe how you can find an initial feasible basis for a feasible LP $\mathcal{P}$, or find if it is infeasible. [10]

(Q4) Use SIMPLEX method to solve the following LP:

$$\begin{aligned} \text{Maximize} \quad & 5x_1 + 4x_2 + 3x_3 \\ \text{subject to} \quad & 2x_1 + 3x_2 + x_3 \leq 5 \\ & 4x_1 + x_2 + 2x_3 \leq 11 \\ & 3x_1 + 4x_2 + 2x_3 \leq 8 \\ & x_1, x_2, x_3 \geq 0 \end{aligned}$$

[10]

(Q5) Solve the following LP:

$$\begin{aligned} \text{Maximize} \quad & x_1 + 2x_2 + x_3 \\ \text{subject to} \quad & x_1 + \tfrac{1}{2}x_2 + \tfrac{1}{2}x_3 \leq 1 \\ & \tfrac{3}{2}x_1 + 2x_2 + x_3 \geq 8 \\ & x_1, x_2, x_3 \geq 0 \end{aligned}$$

[10]

(Q6) (i) Let $\mathcal{D}$ be the dual of $\mathcal{P}$. Show that the dual of $\mathcal{D}$ is $\mathcal{P}$.

(ii) State and prove the weak duality theorem.

(iii) An LP can be any of the following three — feasible and bounded, feasible and unbounded, or infeasible. If the possibilities of the primal $\mathcal{P}$ and the dual $\mathcal{D}$ are paired together, then there can be nine possibilities. Argue with proper reasons which of the nine possibilities can occur.

(iv) Deduce the conditions on A, **b** and **c** so that the primal linear program $\mathcal{P}$ and its dual $\mathcal{D}$ are the same linear program.

[6+5+9+5=25]

(Q7) State and prove the *fundamental theorem* of LP about the relation between an optimal feasible solution and an optimal basic feasible solution. [5+15=20]

INDIAN STATISTICAL INSTITUTE

Mid-Semestral Examination: 2017

12·9·17

Subject Name : **Cryptology**

Course Name : M.Tech. (CS) II yr. Max Score: 40 Duration: 150 Mins

Note: Attempt all questions. Marks are given in brackets. Total score is 50. But maximum you can score is 40. Use separate page for each question.

1. [3+3 = 6] Let $\mathbf{E} = (KG, f, g)$ be a deterministic symmetric-key encryption scheme with message space $\{0,1\}^p$ and ciphertext space $\{0,1\}^c$.

(a) Suppose $p = c$. Is (KG, g, f) always an encryption scheme? Justify your answer.
(b) Is the condition $p = c$ required? Justify.

2.[3+7 = 10] Describe two round Feistel Encryption. Construct an IND-CPA adversary for this?

3. [5+5+5 = 15] Let X, Y be two random variables over S and $f : S \rightarrow S$ be a computable function. Let $\Delta_A(X,Y)$ be defined as $|Pr[A(X) = 1] - Pr[A(Y) = 1]|$. Prove or disprove the following statements:

(a) $TV(f(X), f(Y)) \leq TV(X,Y)$.
(b) For all algorithm A there exists B such that $\Delta_A(f(X), f(Y)) \leq \Delta_B(X,Y)$.
(c) For all algorithm A, $\Delta_A(f(X), f(Y)) \leq \Delta_A(X,Y)$.

4. [2+3+(4+4) = 13] Suppose KG is same as the key-generation of RSA-encryption scheme. We define a new probabilistic encryption algorithm with message $m \leq N/4$ and a random coin $r \in \{0,1,2,3\}$ as $E((e,N), m, r) = (4m + r)^e \mod N$.

(a) Prove that it is an encryption algorithm.
(b) Moreover, construct a decryption algorithm with the soundness property.
(c) Construct a message recovery adversary which can make only one decryption algorithm (note, the decryption algorithm can abort as described in the previous problem). Also compute the success probability of you message recovery algorithm.

5. [6] Let F be a field of size 2^8. Let us define an S-box $S(x) = x^{-1}$ if $x \neq 0$ and $S(0) = 0$. Compute the MDP (maximum differential probability) for the S-box.

INDIAN STATISTICAL INSTITUTE

Semestral Examination : (2017 - 2018)

Course Name : M. Tech. (CS) **Year : 2nd year**

Subject Name : Neural Networks & Applications

Date : September 12, 2017 **Maximum Marks : 50** **Duration : 2 hrs**

Answer all the questions.

1. Show geometrically how a single node perceptron model of artificial neural networks classifies a set of two dimensional patterns distributed in linearly separable two classes. [25]

2. Consider a Multilayer Perceptron (MLP) with two hidden layers for classifying n-dimensional P patterns distributed in k classes. Assume that the numbers of nodes in 1st and 2nd hidden layers are l and m respectively. Derive expressions for amount of updation for the weights, in a single epoch, associated with the links in the MLP, considering batch mode learning. [25]

INDIAN STATISTICAL INSTITUTE

Mid-Semestral Examination : 2014 – 15

MTech CS (2nd Year)

Computational Finance

Date: 12 September 2017 Maximum Marks: 30 Duration: 2 Hours

1. Critically explain the concepts: [2½ X 4 = 10]
    a) Mutual Fund Principle
    b) Law of One Price
    c) Barrier Options
    d) Reflection Principle

2. In the two period model, explicitly solve the Consumption Investment problem for the utility function $u(w) = \ln w$. Compute the relevant expressions and solve for the optimal trading strategy when N = 1, K = 2, r = 1/9, $S_0 = 5$, $S_1(\omega_1) = 20/3$, $S_1(\omega_2) = 40/9$ and $P(\omega_1) = 3/5$, $Q(\omega_1) = 1/2$.

    [8 + 4 = 12]

3. Prove the Put – Call parity of European option for the multi-period market. Is the same relation true for American options? – Prove or refute logically. [5 + 3 = 8]

M. Tech. C. S. II YEAR
Mid-term question paper
Cognitive Science
Date - 12th September, 2017
Instructor: Garga Chatterjee

Time: $1\frac{1}{2}$ hours.

Answer the following questions. Marks for each question are mentioned in bracket after each question. Total marks is 20.

1. Explain the concept of difference threshold and describe the various methods of measuring it by examples. (4)
2. Write briefly about the 3 levels of David Marr's information processing task with respect to vision. (3)
3. At night, we can see big things better than small things. Why? (3)
4. Explain the concept of pitch with respect to sound. (2)
5. Does prolonged exposure to a sub-way (metro/underground) train at 20 feet distance cause hearing loss? (1)
6. What is the difference bwteeen conduction hearing loss and nerve hearing loss? (2)
7. Describe two ways by which depth can be estimated monocularly (using one eye). (2)
8. How are 'greebles' like faces? (3)

INDIAN STATISTICAL INSTITUTE

Semestral Examination:(2017-2018)

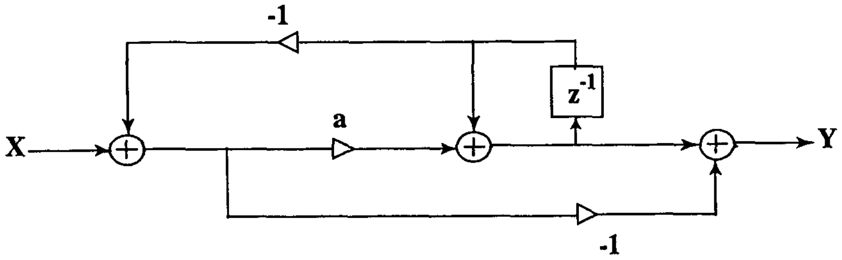
MTech C.S. 2nd Year

Digital Signal Processing

Date: 17.11.2017 Maximum Marks: 100 Duration: 3 hours

Note: The examination is open book, open notes. The marks add up to 114. The maximum you can score is 100. Use of calculators is permitted.

1. (a) Obtain the system function $H(z)$ of the structure shown below. Also, determine and justify if it can be used as an all-pass filter.



(b) Assuming a two's complement fixed point representation with all numbers in fractional form and a wordlength of 4 bits (1 bit for the sign), calculate the output noise variance due to product round-off. Assume that the '-1' multipliers do not contribute to the roundoff noise.

(c) Give a Direct Form II representation of a cascade of two systems, each with system function $H(z)$.

[(7+3)+10+3=23]

2. The 4-point Discrete Fourier Transform (DFT) of a length-4 complex sequence $v[n] = x[n] + jy[n]$ is:

V[0]=-2+j6, V[1]= 3+j5, V[2]=6+j4, V[3]=-1+j8

where $x[n]$ and $y[n]$ are the real and imaginary parts of $v[n]$, respectively. Without computing the IDFT of $V[k]$, determine the 4-point DFTs $X[k]$ and $Y[k]$ of the real sequences $x[n]$ and $y[n]$. [10]

3. Consider a system with system function

$$H(z) = \frac{0.3 + z^{-1}}{1 + 0.5z^{-1}}$$

   (a) Assuming a causal system, sketch its region of convergence (ROC). Suggest a modification of this system which would have minimum phase but have the same magnitude response as the original system.

   (b) Give a Parallel Form representation of the overall system.

[(3+5)+5=13]

4. An ideal analog lowpass filter has a frequency response given by

$$H_a(j\Omega) = \begin{cases} 1, & |\Omega| < \Omega_c, \\ 0, & otherwise \end{cases}$$

Let $H_1(e^{j\omega})$ and $H_2(e^{j\omega})$ be the frequency responses of digital filters obtained by sampling the impulse response of the analog filter at sampling rates $T_1 = 3\pi/2\Omega_c$ and $T_2 = \pi/\Omega_c$, respectively. Assume that $H_1(e^{j0}) = H_2(e^{j0}) = 1$. Sketch the frequency response of the system $H(z) = H_1(z) - H_2(z)$ and comment on its nature. [10+2]

5. Let $Y[k]$ denote the MN-point DFT of a length-N sequence $x[n]$ appended with $(M-1)N$ zeros. Suggest how you would obtain $X[k]$ from $Y[k]$. [8]

6. The linear convolution of a length-80 sequence with a length-250 sequence is to be computed using 128-point DFTs and IDFTs. Determine the minimum number of DFTs and IDFTs required to perform the computation using the overlap-add approach. [8]

7. Consider a sequence $g[n] = n(0.4)^n, \quad n \geq 0$ with a Discrete Time Fourier Transform (DTFT) $G(e^{j\omega})$ and z-transform $G(z)$.

   (a) Without evaluating $G(e^{j\omega})$, determine the inverse DTFT of $jIm\{G(e^{j\omega})\}$.

   (b) Determine $G(z)$ and sketch its poles and zeros. [5+5]

8. Using Parseval's relation, evaluate $\int_0^\pi \frac{4}{(1.04-0.4cos\omega)}d\omega$. [5]

9. A causal LTI system is described by the difference equation:

$$y[n] = b_0x[n] + b_1x[n-1] - a_1y[n-1] - a_2y[n-2]$$

Determine the difference equation representation of its inverse system. [5]

10. Determine the impulse response coefficients of a Type I FIR filter of length 5 so that for an input $x[n] = cos(0.3n) + cos(0.4n) + cos(0.7n)$, only the mid-frequency component passes through. [8]

11. Develop a flow-graph for a radix-3 Decimation-in-Frequency FFT algorithm for N=9. [12]

Indian Statistical Institute

Semestral Examination: 2017
M. Tech. in Computer Science
Mobile Computing
M. Tech - II year

Date: 17-11-2017 | Maximum Marks: 100 | Duration: 3 hours

Instructions: You **may** attempt all questions which carry a total of **110** marks. However, the maximum marks you can score is only **100**.

1. (a) State the differences between fixed spectrum access and dynamic spectrum access techniques in cognitive radio networks. [6]

   (b) What are the roles of sensing channel and reporting channel in cooperative spectrum sensing in cognitive radio networks? [7]

   (c) Explain with an example the relay-assisted cooperative spectrum sensing technique in cognitive radio networks. [7]

2. (a) Explain the concept of *request zone* as defined in the location-aided routing (LAR) protocol for adhoc networks. If a request zone is rectangular in shape, how does a node determine if it is in the request zone for a particular route request? [4+6]

   (b) What is bordercasting? [4]

   (c) Explain the concept of *routing zone* as defined in the zone routing protocol (ZRP) in an adhoc network. [6]

3. (a) What is attribute-based addressing in wireless sensor networks? [3]

   (b) State the main difference between self-diagnosis and cooperative diagnosis based fault detection techniques in wireless sensor networks. [4]

   (c) Consider a linear network consisting of n sensor nodes and the base station (BS) as shown in Figure 1 where the distance between two consecutive nodes is r. The distance between the last node n and the BS is also r. Circles denote the sensor nodes and the square denotes the BS.

      i. Derive expressions for total energy expended in the system for transmitting a k-bit message from node 1 to the BS using direct communication and minimum transmission energy (MTE) routing protocols. [4+4]

      ii. Under what condition does direct communication routing require less energy than MTE routing in wireless sensor networks? [2]

   (d) Describe how randomized rotation of cluster-heads is used to evenly distribute the energy load among the sensors in the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol in wireless sensor networks. [8]

P. T. O

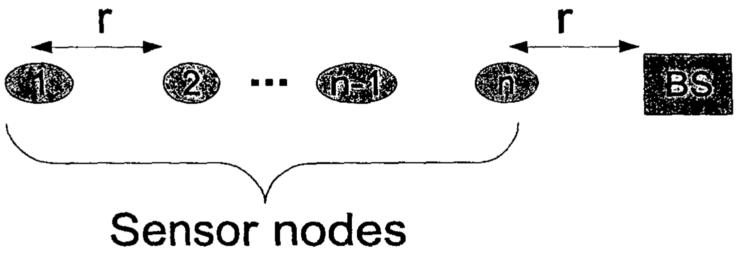


Figure 1: Linear network with n nodes and the base station.

(e) Present an approximation algorithm for the following minimum relay node placement problem in wireless sensor networks:

Given a set of sensor nodes S with their locations and an uniform communication radius d of both sensor and relay nodes, the problem is to place a set of relay nodes R such that the whole network G consisting of both sensor and relay nodes is *2-connected*. The objective of the problem is to minimize $|R|$, where $|R|$ denotes the number of relay nodes in R. [10]

4. (a) State the fundamental difference between *macrocell tier* and *device tier* communications in 5G cellular network. [5]

(b) Compare the *closed access* and *open access* mechanisms used for providing security to the devices that operate in the device tier of 5G cellular networks. [5]

(c) Formulate the joint mode selection, channel assignment and power control problem in device-to-device (D2D) communication in 5G cellular networks as a mathematical optimization problem. Explain your optimization formulation briefly. [12]

(d) State two fundamental propagation features in millimeter wave D2D communication. [5]

(e) Compare *maximum rate* and *full utilization* session admission policies in cellular networks. [4+4]

INDIAN STATISTICAL INSTITUTE

First Semester Examination: 2017-18

M. Tech.(CS) – II Year, (Semester - IV)

Optimization Techniques

Date: 20.11.2017 Maximum Marks: 100 Duration: 3.5 Hours

Note: The question paper is of 115 marks. Answer as much as you can, but the maximum you can score is 100.

Vectors are written in lower case with boldface, e.g., $\mathbf{b}$, the j-th entry of the vector $\mathbf{b}$ is denoted by b_j. Matrices are written in upper case, e.g., A; the (i, j)-th entry of the matrix A is denoted by a_{ij}. Transpose of A is denoted by A^T, and transpose of $\mathbf{b}$ is denoted by $\mathbf{b}^T$. A is an $m \times n$ $(m \leq n)$ matrix of reals, and is of rank m, $\mathbf{b} \in \mathbb{R}^m$, $\mathbf{c} \in \mathbb{R}^n$ and $\mathbf{x} \in \mathbb{R}^n$. $\mathcal{P}$ will denote a linear program of the form

$$\begin{array}{rl} \text{Maximize} & \mathbf{c}^T\mathbf{x} \\ \text{subject to} & A\mathbf{x} \leq \mathbf{b} \\ & \mathbf{x} \geq \mathbf{0} \end{array}$$

and $\mathcal{P}_{eq}$ will denote a linear program of the form

$$\begin{array}{rl} \text{Maximize} & \mathbf{c}^T\mathbf{x} \\ \text{subject to} & A\mathbf{x} = \mathbf{b} \\ & \mathbf{x} \geq \mathbf{0} \end{array}$$

(Q1) Let G be a connected undirected graph with n vertices. Design a mathematical program that computes the minimum spanning tree of G. Explain your mathematical program with suitable justifications. [6+4=10]

(Q2) Consider $\mathcal{P}_{eq}$, where all entries of A, $\mathbf{b}$ and $\mathbf{c}$ are integers. Let $X = \{x_1, \dots, x_j, \dots, x_n\}$ be a basic feasible solution. Then, prove that $|x_j| \leq m!\ \alpha^{m-1}\beta$, where $\alpha = \max_{i,j}\{|a_{ij}|\}$ and $\beta = \max_{j=1,\dots,m}\{|b_j|\}$. [10]

(Q3) Prove that $\mathcal{P}$ has an optimal solution if and only if the following set of constraints has a feasible solution.

$$\begin{array}{rcl} A\mathbf{x} & \leq & \mathbf{b} \\ A^T\mathbf{y} & \geq & \mathbf{c} \\ \mathbf{c}^T\mathbf{x} & \geq & \mathbf{b}^T\mathbf{y} \\ \mathbf{x}, \mathbf{y} & \geq & \mathbf{0} \end{array}$$

[10]

(Q4) Let $P, Q \subseteq \mathbb{R}^n$ be convex sets and let $f : \mathbb{R}^n \to \mathbb{R}$ be a strictly convex function. Suppose that x^* is an optimum solution to $\min\{f(x) \mid x \in P \cap Q\}$ and x^* lies in the interior of Q. Show that x^* is also an optimum solution to $\min\{f(x) \mid x \in P\}$. [10]

(Q5) (i) Define a *totally unimodular* matrix (TUM).

(ii) Let A be a TUM. Is $[A|A]$ a TUM? If yes, prove it. Else, give a counterexample.

(iii) Consider an LP of the form $\mathcal{P}$, where $\mathrm{b} \in \mathbb{Z}^m$. If A is TUM, and if $\mathcal{P}$ has an optimal solution, then show that it also has an integral optimal solution $\mathrm{x}^* \in \mathbb{Z}^n$.

[2+5+8=15]

(Q6) Player A has a red card of value 8 and a blue card of value 1. Player B has a red card of value 2 and a blue card of value 7. The players simultaneously choose a card to play. If the chosen cards are of the same color, Player A wins. Player B wins if the cards are of different colors. The amount won, in rupees, is equal to the number on the winners card. Compute the payoff matrix, the value of the game and the optimal mixed strategies of the players. [5+3+12=20]

(Q7) (a) State Farkas lemma.

(b) State the strong duality theorem.

(c) Use Farkas lemma to prove the strong duality theorem.

[1+1+8=10]

(Q8) Describe an interior point method for solving an LP of the form $\mathcal{P}_{eq}$. You can assume that an initial feasible point inside the feasible polyhedron corresponding to the LP has been given to you. Your description of the algorithm should include the following:

- the barrier function and the auxiliary problem it generates,
- derivation of the necessary conditions for the existence of a unique maximizer for the auxiliary problem,
- the steps of the algorithm and the number of iterations performed.

[(2+2)+10+(4+2)=20]

(Q9) We are given a steel sheet of area 54 square metres. Our job is to construct a box of maximum volume from this sheet.

- Formulate the problem as a mathematical program.
- Using Lagrangian multiplier, or otherwise, solve the mathematical program.

[3+7=10]

INDIAN STATISTICAL INSTITUTE

First Semester Examination: 2017-18

M. Tech.(CS) – II Year, (Semester - IV)

Optimization Techniques

Date: 20.11.2017 Maximum Marks: 100 Duration: 3.5 Hours

Note: The question paper is of 115 marks. Answer as much as you can, but the maximum you can score is 100.

Vectors are written in lower case with boldface, e.g., $\mathbf{b}$, the j-th entry of the vector $\mathbf{b}$ is denoted by b_j. Matrices are written in upper case, e.g., A; the (i,j)-th entry of the matrix A is denoted by a_{ij}. Transpose of A is denoted by A^T, and transpose of $\mathbf{b}$ is denoted by $\mathbf{b}^T$. A is an $m \times n$ $(m \leq n)$ matrix of reals, and is of rank m, $\mathbf{b} \in \mathbb{R}^m$, $\mathbf{c} \in \mathbb{R}^n$ and $\mathbf{x} \in \mathbb{R}^n$. $\mathcal{P}$ will denote a linear program of the form

$$\begin{aligned} \text{Maximize} \quad & \mathbf{c}^T\mathbf{x} \\ \text{subject to} \quad & A\mathbf{x} \leq \mathbf{b} \\ & \mathbf{x} \geq \mathbf{0} \end{aligned}$$

and $\mathcal{P}_{eq}$ will denote a linear program of the form

$$\begin{aligned} \text{Maximize} \quad & \mathbf{c}^T\mathbf{x} \\ \text{subject to} \quad & A\mathbf{x} = \mathbf{b} \\ & \mathbf{x} \geq \mathbf{0} \end{aligned}$$

(Q1) Let G be a connected undirected graph with n vertices. Design a mathematical program that computes the minimum spanning tree of G. Explain your mathematical program with suitable justifications. [6+4=10]

(Q2) Consider $\mathcal{P}_{eq}$, where all entries of A, $\mathbf{b}$ and $\mathbf{c}$ are integers. Let $X = \{x_1, \ldots, x_j, \ldots, x_n\}$ be a basic feasible solution. Then, prove that $|x_j| \leq m!\ \alpha^{m-1}\beta$, where $\alpha = \max_{i,j}\{|a_{ij}|\}$ and $\beta = \max_{j=1,\ldots,m}\{|b_j|\}$. [10]

(Q3) Prove that $\mathcal{P}$ has an optimal solution if and only if the following set of constraints has a feasible solution.

$$\begin{aligned} A\mathbf{x} &\leq \mathbf{b} \\ A^T\mathbf{y} &\geq \mathbf{c} \\ \mathbf{c}^T\mathbf{x} &\geq \mathbf{b}^T\mathbf{y} \\ \mathbf{x}, \mathbf{y} &\geq \mathbf{0} \end{aligned}$$

[10]

(Q4) Let $P, Q \subseteq \mathbb{R}^n$ be convex sets and let $f : \mathbb{R}^n \to \mathbb{R}$ be a strictly convex function. Suppose that x^* is an optimum solution to $\min\{f(x) \mid x \in P \cap Q\}$ and x^* lies in the interior of Q. Show that x^* is also an optimum solution to $\min\{f(x) \mid x \in P\}$. [10]

INDIAN STATISTICAL INSTITUTE

Semestral Examination:(2017-2018)

M.TECH (CS) II YEAR

Subject Name: Quantum Information Processing and Quantum Computation

Maximum Marks: 60 Duration: 3 hours Date: 24.11.2017

Answer any five of the following questions

1. a) Consider the following three-qubit state shared between Alice, Bob and Charlie stationed at distant laboratories;

$$|\psi\rangle_{ABC} = \frac{1}{\sqrt{3}}|000\rangle + \frac{\sqrt{2}}{\sqrt{3}}|111\rangle$$

$|0\rangle$ and $|1\rangle$ form an orthonornal basis in two dimensional Hilbert space.

i) Find the maximum probability of transforming the state to a three-qubit maximally entangled state by local operations and classical communication.
ii) Show that Alice can help to create the Bell state $|\phi^+\rangle$ between Bob and Charlie out of the three-qubit maximally entangled state where all of them are allowed to do local operation and classical communication.
b) Let Alice, Bob and Charlie share a three-qubit maximally entangled state and in addition Alice and Dick share a entangled state $|\psi\rangle = a|00\rangle + b|11\rangle$. Show how the the state shared between Alice and Dick can be transferred to Bob and Charlie by local operation and classical communications.
[2+3+7]

2. a) Let a single qubit unitary gate U be realized in the following way;

$$U = A\sigma_x B\sigma_x C$$

where A, B and C are also single qubit gates with $ABC = I$ Show using diagram, how two-qubit gate $C - U$ can be implemented by single qubit gates and $C - NOT$ gates.

b) Let V and U are two gates where $U = V^2$. Draw the circuit diagram and analyze how the two-qubit $C^2 - U$ can be implemented by elementary gates.
c) Show that $[\sigma_x \otimes \sigma_x, \sigma_z \otimes \sigma_z] = 0$. Find the joint measurement results of the two observables $\sigma_z \otimes \sigma_z$ and $\sigma_x \otimes \sigma_x$ on the two-qubit state $|\phi^-\rangle = \frac{1}{\sqrt{2}}[|00\rangle - |11\rangle]$ by using the measurement circuit.

[4+4+4]

3. a) Consider a function $f : \{0,1\}^n \rightarrow \{0,1\}$, where the function f is either constant or balanced ($f(x) = 0$ for half of the possible input values). Describe the quantum algorithm by which the function can be shown to be either constant or balanced without calculating the function at various points.

b) Consider a function $f_a : \{0,1\}^n \rightarrow \{0,1\}$ where the function f_a is given by $f_a(x) = x.a$, a being a n-bit string. Describe the quantum algorithm by which a can be determined.

[8+4]

4. The function $f : \{0,1\}^n \rightarrow \{0,1\}$ is such that:
$f(x) = 1$, for $x = \omega$ and $f(x) = 0$ for $x \neq \omega$
a) Discuss how many queries are required for finding ω in classical case.
b) Discuss the quantum algorithm that provides a quadratic speed up for this search problem.

[2+10]

5. Consider a 2 to 1 function $f : \{0,1\}^n \rightarrow \{0,1\}^n$. The function has a period given by n-bit string a: that is
$f(x) = f(y)$ iff $y = x \oplus a$
a) Discuss how hard it is to find the period a in the classical world.
(b) Discuss the quantum algorithm by which the period can be found in polynomial time.

[2+10]

6. (a) Discuss how the following quantum Fourier Transform can be im-

plemented by using single qubit and two-qubit gates;

$$QFT : |x\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle$$

(b) Using the solution of the last problem provide a sketch of the quantum algorithm for finding the prime factors of a large number.

[4 + 8]

7.(a) Show that the following two five qubits states:

$$|0_L\rangle = \frac{1}{4}[|00000\rangle+|10010\rangle+|01001\rangle+|10100\rangle+|01010\rangle-|11011\rangle-|00110\rangle-|11000\rangle$$
$$-|11101\rangle-|00011\rangle-|11110\rangle-|01111\rangle-|10001\rangle-|001100\rangle-|10111\rangle+|00101\rangle]$$
$$|1_L\rangle = \frac{1}{4}[|11111\rangle+|01101\rangle+|10110\rangle+|01011\rangle+|10101\rangle-|00100\rangle-|11001\rangle-|00111\rangle$$
$$-|00010\rangle-|11100\rangle-|00001\rangle-|10000\rangle-|01110\rangle-|10011\rangle-|01000\rangle+|11010\rangle]$$

are stabilized by the following four operators;

$$M_1 = XZZXI, M_2 = IXZZX, M_3 = XIXZZ, M_4 = ZXIXZ$$

where X, Y, Z represnt the Pauli operators I is the identity operator.
(b) Show that by using this five-qubit quantum code and by measuring the above mentioned observables, any one-qubit error can be corrected.

[3 + 9]

INDIAN STATISTICAL INSTITUTE

First Semester Examination: 2017-18

M. Tech. (Computer Science) Second Year

Natural Language Processing

Date: 22. 11. 2017 Maximum Marks: 50 Duration: 2 h 30 min

NOTE: **Total Marks: 60,** Answer all questions.

---

1. (Related to Lemmatization)

An edit tree encodes the transformation between two strings. To extract an edit tree for a source-target string pair <*s*, *t*>, at first the longest common substring (LCS) is found between them and then recursively the prefix and suffix pair of the LCS are modelled. When no LCS is found between <*s*, *t*>, the string pair is represented as a substitution operation transforming the first string to the second. The resulting edit tree does not encode the LCSs but only the length of their prefix and suffix and the substitution nodes. For example, the edit tree between the source-target strings 'umgeschaut'-'umschauen' is given in figure 1.

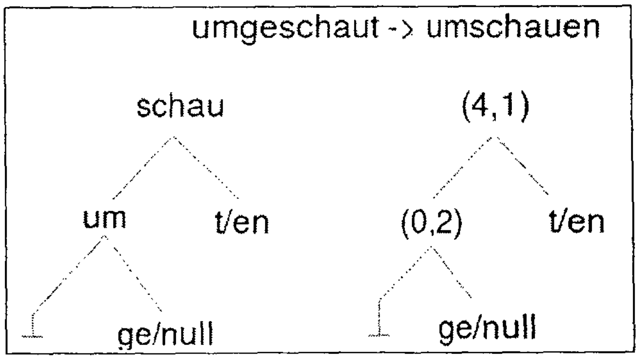


Figure 1. An example edit tree

Write down pseudo code for finding the edit tree between two strings (x, y). Given that:

(i) LCS(x, y) returns a 4-tuple (x_s, x_e, y_s, y_e), where x_s and x_e are start and end index of the LCS in x and y_s and y_e are start and end index of the LCS in y. It returns NULL is no LCS is found.

(ii) Length() returns the length of a given input string.

[10]

2. (Related to word embedding)

(a) Explain hierarchical softmax and negative sampling in Continuous Bag of Words (CBOW) and skipgram models.

(b) Why are negative samples needed in negative sampling?

[(3 + 3) + 4 = 10]

3. (Related to RNN and LSTM)

(a) Explain vanishing/exploding gradient problem in the context of Recurrent Neural Network (RNN).

(b) What is gradient clipping? Can a similar technique be used to deal with vanishing gradient problem?

(c) In RNN, the output of the hidden layer at time t, h_t, can be written as $h_t = f(x_t, h_{t-1})$ where x_t is the input at time t. Suppose skip connections are added to the RNN architecture so that $h_t = f(x_t, h_{t-1}) + h_{t-2}$. How will adding skip connections affect the vanishing gradient problem?

(d) Explain, using diagrams, the selective read/write operations in the LSTM architecture.

[5 + 5 + 5 + 5 = 20]

4. (Related to Named Entity Recognition and Machine Translation)

(a) Consider two NER systems, one based on the use of word embedding and the other using both word and character embedding jointly. Which model do you think is better for NER task? Explain your answer with a suitable illustration.

(b) Consider a Bengali to Hindi machine translation system which does word-wise translation due to resource constraint. Here is an example:

Bengali: ফুলে ফুলে বাগান ভরে গেছে| (/phule /phule /bAgAn /bhore /gechhe)

Word wise translation: ফুলে/phule → फूल मे; ফুলে/phule → फूल मे; বাগান/bAgAn → बगीचा; ভরে/bhore → भरके; গেছে/gechhe → गया ;

So the translation in Hindi becomes: फूल मे फूल मे बगीचा भरके गया| However, the actual translation should have been: फूलों से बगीचा भर गया|

What minimum additional NLP resource(s) would you require to produce the correct translation for the above example? Explain your answer.

[5 + 5 = 10]

5. (Probabilistic CFG)

Consider a simple Probabilistic Context Free Grammar (PCFG) as given below. The non-terminals are S, NP, PP, VP, P, and V. The start symbol is denoted by S. The terminals are the words in italics.

S	→	NP VP	1.0	NP	→	NP PP	0.4
PP	→	P NP	1.0	NP	→	*astronomers*	0.1
VP	→	V NP	0.7	NP	→	*ears*	0.18
VP	→	VP PP	0.3	NP	→	*saw*	0.04
P	→	*with*	1.0	NP	→	*stars*	0.18
V	→	*saw*	1.0	NP	→	*telescopes*	0.1

Using the above grammar, two different parses of the sentence, `astronomers saw stars with ears`, are possible. Show these two parses and compute the probabilities of these two parses. Compute the sentence probability.

[(2 + 2) + (2+2) + 2 = 10]

Indian Statistical Institute

M.Tech (CS) II

Information and Coding Theory

Semester Examination

Maximum Marks: 100

Date: November 22, 2017
Time 3 hours

The question paper contains 8 questions. Total marks is 105. Maximum you can score is 100. Unless otherwise mentioned, all notations are the same as presented in class

1. Let $\mathcal{C}$ be a linear code.

   (a) Show that $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$.

   (b) If $\mathcal{C} + \mathcal{D} = \{u + v : u \in \mathcal{C}, v \in \mathcal{D}\}$, then show that $(\mathcal{C} + \mathcal{D})^{\perp} = (\mathcal{C})^{\perp} + (\mathcal{D})^{\perp}$.

   (5 + 5 = 10)

2. Prove that for a t-error-correcting code of length n over a field with q elements and containing M codewords, the following relation holds.

$$M(1 + (q-1)\binom{n}{1} + \cdots + (q-1)^t\binom{n}{t}) \leq q^n.$$

   (5)

3. What is a perfect code? Show that the binary repetition code is not a perfect code. (5)

4. (a) Construct a BIBD using H_8. What are the parameters of the design?

   (b) Construct a Hadamard matrix of order 12.

   (c) Construct a $(7, 16, 8)$ Hadamard code. (5+10+10=25)

5. What are MDS codes? Prove that Reed-Solomon codes are MDS linear codes. Write a decoding algorithm for Reed-Solomon codes and prove the correctness of the algorithm.

   (2 + 5 + 6 + 10 = 23)

6. Consider a triple-error correcting binary BCH code of length 15. What are the parameters of the code? Write the (a) generator polynomial (b) parity check matrix of the code.

   (2 + 10 + 5 = 17)

7. Construct a $(5, 2)$-Cauchy-Reed-Solomon code over $GF(2^4)$. (10)

8. Let $\mathcal{C}$ be a cyclic code of length n, which is an ideal in $R_n = F[x]/(x^n - 1)$. Show that there is a unique monic polynomial $g(x)$ of minimal degree in $\mathcal{C}$ and that this polynomial is the generator polynomial of $\mathcal{C}$. What is the generator matrix of $\mathcal{C}$? (3 + 3 + 4 = 10)

INDIAN STATISTICAL INSTITUTE

First Semester Examination: 2017-2018

M. Tech (CS) - II

Computational Geometry

Date : 24.11.2017 Maximum Marks : 50 Duration : 2 hrs 30 minutes

(Although the paper carries a total marks of 60, the maximum marks you can score is 50)

Question 1: (a) In Meggido's prune and search algorithm, if the center of minimum enclosing disk is constrained to lie on the x-axis then which are the points, in Figure 1, will get pruned after first iteration for the given pairing of the points. The bisectors of the pairs are shown in the figure 1. [5]

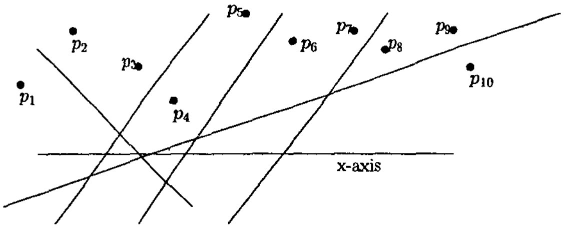


Figure 1:

(b) List the ordered set of points deleted from the stack by Graham Scan algorithm for computing the upper envelope of the convex hull of the point set shown in Figure 2. [5]

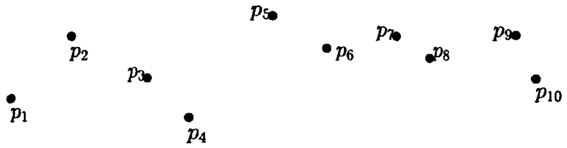


Figure 2:

P.T.O

Question 2: (a) Construct a simple polygon P and a placement of guards such that the guards taken together can see every point on the boundary of P but there is at least one point in the interior of P that is not visible to the guards. [5]

(b) Prove that the line segment between a closest pair of points in a point set P is an edge of the Delaunay triangulation of P. [5]

Question 3: Given a partition $\mathcal{P}$ of a 2D space build for balanced k-D tree of n points using the alternating splitting rule. Prove that any vertical or horizontal line stabs $O(\sqrt{n})$ cells of $\mathcal{P}$. [10]

Question 4: Given a set P of n points in the plane. Give an $O(n^2)$ time algorithm to determine the minimum area triangle whose vertices are selected from P. [10]

Question 5: Given a set P of n points in R^d. Give an $O(n \log n)$ time algorithm to find closest pair of points in P, when d is a constant. [10]

Question 6: Given a range space $S = (X, R)$, where $|X| = n$ and R is a family of subsets of X. If VC-dimension of S is δ then prove that $|R|$ is bounded by n^δ. [10]

INDIAN STATISTICAL INSTITUTE

First Semester Examination: 2017-18

Name and Year of Programme: MTech Computer Science [2nd Year]

Name of Course: Cognitive Science

Date: 25/11/2017 Maximum Marks: 80 Duration : 180 minutes

Answer any 16 of the following 18 questions.

1. Explain serial processing and parallel processing in a cognitive system with any example. [5]
2. If the fMRI activation in a part [say Part A] of the brain is observed and if Part A of the brain is associated with Function B, can one say that fMRI activation of Part A means that Function B being ongoing? Explain. [5]
3. Can we take an one time EEG reading? What are the advantages of averaging EEG signal outputs? [5]
4. What does the Phineas Gage incident tell us about general functionality versus specific functional modules or specificity of the human brain system? [5]
5. If you are in a crowded room and you suddenly hear your name, you hear it but you don't always know when other things are being said, which you are not attending to. Why is this the case? [5]
6. Explain the Flanker Task [Posner 1984]. What does it tell us about attention system? [5]
7. In information theoretical terms as well as cognitive science, what is chunking? Explain with an example. [5]
8. What are primacy and recent effects in short term memory? [5]
9. What is binocular rivalry? Describe any two different types of binocular rivalry based on stimulus property type. [5]
10. Describe pop-out and conjunction search with graphs and plots. [5]
11. What is REM sleep? What happens to duration of REM sleep as night goes on? [5]
12. What are hypersomnia and sleep apnoea? [5]
13. Why does the sensory homunculus look like the way it does – what explains the proportional shape of its parts? [5]
14. Explain consciousness from the stand-point of complexity theory. [5]
15. Explain the usual method of lie detection and why it is not full proof. [5]
16. Explain what is a Hebbian synapse. [5]
17. Explain inattentional blindness. [5]
18. Explain the basic principles underlying electro encephalogram and functional magnetic resonance imaging. [5]

INDIAN STATISTICAL INSTITUTE

Semestral Examination : (2017 - 2018)

Course Name : M. Tech. (CS) **Year : 2nd year**

Subject Name : Neural Networks & Applications

Date : November 27, 2017 **Maximum Marks : 100** **Duration : 3 hrs 30 mins**

Answer all the questions.

1. (a) State the Hadamard's conditions for a problem to be well-posed.

   (b) How is Tikhonov's Regularization Theory used for solving ill-posed problems?

   (c) In the context of artificial neural networks, give an example of a widely used regularizer. Explain how this regularizer is incorporated, according to Tikhonov's Regularization Theory, in the objective function.

   (d) What are the physical significances of the situations when the regularization parameter $\lambda \to 0$ and $\lambda \to \infty$? [5 + 5 + 5 + 2 = 17]

2. (a) What is the utility of an Autoencoder?

   (b) Consider a Stacked Sparse Autoencoder.

   i) State and explain an expression for reconstruction error along with appropriate regularizer for a data set to be fed to the above Stacked Sparse Autoencoder.

   ii) Write down the sparsity penalty for this autoencoder.

   iii) Explain how this autoencoder is trained with a data set. [2 + 5 + 7 + 6 = 20]

3. (a) Explain the advantages of Convolutional Neural Networks over Multilayer Perceptrons for classifying a set of multichannel images.

   (b) Explain with an appropriate example whether convolution operation is equivariant under translation and shifting.

   (c) State and explain the learning rule for training a Convolutional Neural Network.

   [4 + 3 + 13 = 20]

4. (a) Consider the 2-input XOR problem in the domain of pattern classification. Show that a linear model is not appropriate for designing a classifier for this problem.

(b) Consider a Multilayer Perceptron (MLP) with one hidden layer consisting of two nodes, and an output node. Assume that the activation function for each hidden node is ReLU while that for the output node is linear. The bias values for the hidden nodes constitute the vector $\mathbf{c} = [0, -1]^T$, while that for the output node is $b = 0$. The weight vector of the synaptic connections between the output layer and the hidden layer is $\mathbf{w} = [1, -2]^T$. The value of each of the connection weights between input and hidden nodes is 1. Show with detailed enumeration how the MLP is able to classify all the inputs. [10 + 10 = 20]

5. Consider a dynamical system driven by an n-dimensional external signal $\mathbf{x}(t)$ such that

$$\mathbf{s}(t) = \mathbf{f}(\mathbf{s}(t\text{-}1), \mathbf{x}(t); \boldsymbol{\theta}_1),$$

where $\mathbf{s}(t)$ is the state of the system at time t, and $\boldsymbol{\theta}$ constitutes the parameters of the function $\mathbf{f}$. The output of the system at time t is

$$\mathbf{y}(t) = \mathbf{g}(\mathbf{s}(t); \boldsymbol{\theta}_2),$$

where $\boldsymbol{\theta}_2$ constitutes the parameters of the function $\mathbf{g}$.

(a) Design an appropriate artificial neural network for modeling this dynamical system.

(b) Derive its learning rule. [5 + 23 = 28]

INDIAN STATISTICAL INSTITUTE

First Semester Examination: 2017-18

M.Tech CS II

Artificial Intelligence

Date: 27/11/2017 Maximum Marks: 100 Duration: 3 Hours

Answer any 5 Questions

1) Let S={~PV~R, PVR, ~PVR, PV~RVQ, QVR, PV~RV~Q}. [20]

Construct the closed semantic tree of the set of clauses S.

2) According to Herbrand's Theorem ; A set S of clauses is unsatisfiable if and only if there is a finite unsatisfiable set S' of ground instances of clauses of S. [20]
Let S={P(x), Q(x,f(x))V~P(x), ~Q(g(y),z)}.

Determine S' of S as stated above.

3) Determine the most generalised unifier (mgu) of the following two predicates: [20]
P1=P(x,g(x),y) and P2=P(z,u,g(u)).

4) Premises: The members of the selection committee test the performance of everyone who enters the cricket team for the first time and who is not a regular test cricketer. Some previous test cricketers enter the cricket team and their performances are only tested by previous test cricketers. No previous test cricketer is regular test cricketer. [20]

Let L(x) mean 'x enter the cricket team', U(x) mean 'x is a regular test cricketer'. T(x,y) mean 'y test the performance of x', M(x) mean 'x is a member of the Selection committee' and R(x) mean 'x is a previous test cricketer'.

Draw the conclusion that some of the committee members are previous test cricketers.

5) Consider the following expressions [20]
$(\forall x)(\forall y)(\forall z)[Parent(x,z)\Lambda parent(z,y) \rightarrow Grandparent(x,y)]$

$(\forall x)(\forall y)[Mother(x,y) \rightarrow Parent$(x,y)]

$(\forall x)(\forall y)[Father(x,y) \rightarrow Parent$(x,y)]

Father(Zeus, Ares)

Mother(Hera, Ares)

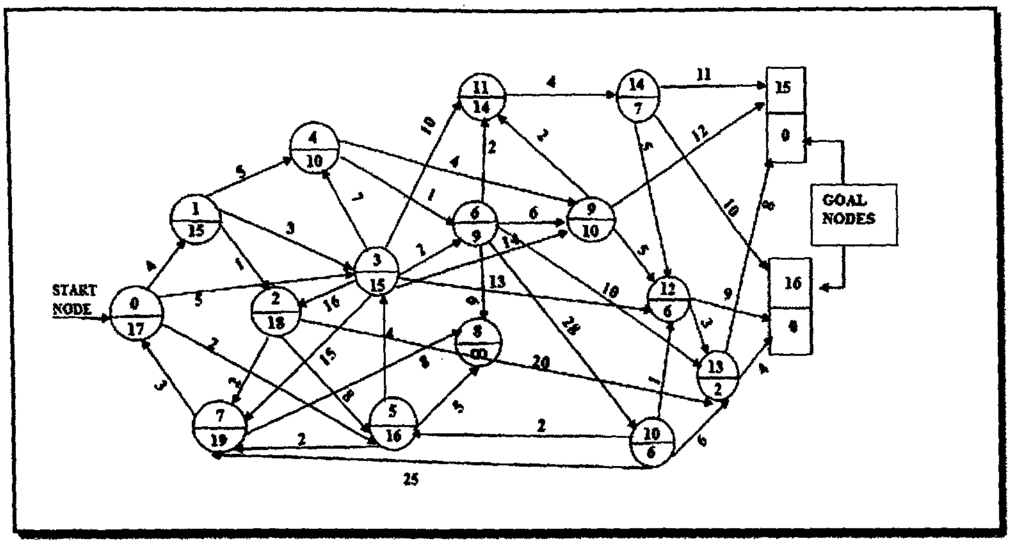
Father(Ares, Harmonia).

From the above facts and rules of a deductive database system answer the following question;

Is there a grandparent of Harmonia?

P.T.O

6) Consider the following OR graph. [20]



Each node n of the graph represents {cost of the node n/admissible heuristic of node n}.

Apply A* Search algorithm and determine the optimal path of the graph.

7) There are two jugs of two different capacities. One is of 3-gallon capacity and the other one is of 4-gallon capacity. Initially both the jars are empty. There is an external source of water (tap). The goal is to fill the 4-gallon jug with exactly 2-gallons of water.

The state is described in the following manner:

(Volume of water in 4-gallon jug, Volume of water in 3-gallon jug). The initial state is quite obvious from the statement of the problem.

i) Determine the Possible set of states of water jug problem along with start state and goal states. [10]

ii) Considering the constraints of the problem determine how to end up pouring exactly 2-gallon of water in the 4-gallon jug. [10]

INDIAN STATISTICAL INSTITUTE

First Semester Examination: (2017 – 2018)

M.Tech. (CS) II Year

Parallel Processing: Architectures and Algorithms

Date: 27 /11/2017 Total Marks: 120 Duration: 3 hrs

NOTE: You may answer all questions but the maximum mark you may score is 100.

1. a) State Bernstein's conditions for parallelism.

b) For a given problem size of interest, *6* percent of the operations of a parallel program are inside I/O functions that are executed on a single processor. Find the minimum number of processors needed for the parallel program to exhibit a speed-up of 10.

c) Consider the following program segment with seven instructions:

I_1 : B = B + C
I_2 : D = B * A
I_3 : E = B + C
I_4 : F = A + C
I_5 : A = E + D
I_6 : C = E * A
I_7 : B = E * F

Based on data dependency, draw the program flow graph considering each statement as a process. Show a possible scheduling assuming as many processors as needed. Assume that the operations '+', '*', and inter-process communication take 10, 40 and 30 time units respectively. Calculate the speed-up and utilization achieved by your parallel scheduling.

[3+6+(6+6+5) = 26]

2. a) Given *m* sets of numbers, each containing *n* elements: $S_j = \{x_{j1}, x_{j2}, \ldots \ldots, x_{jn}\}$, $1 \leq j \leq m$, and *n* is a power of 2, it is required to find the sum of each set: $SUM_j = \sum_k x_{jk}$, $1 \leq k \leq n$. Develop a parallel architecture that can produce the results in $(\log n + m - 1)$ steps only.
Find *N*, the number of processors required and what will be the interconnection network? Mention the initial input data distribution and the delivery of output.

b) Is it possible to implement the above algorithm using nearly *N/2* number of processors connected by a hypercube network without any slow down? If possible, show a scheme for many-to-one embedding of the network used in (a) on the hypercube, for *n=8*.

[(10 + 5) + (3 + 6) = 24]

P.T.O

3. Explain how the Newton's method for solving non-linear equations can be implemented efficiently on a CRCW SM (*concurrent-read-concurrent-write shared memory*) MIMD computer to solve the equation $f(x) = 0$. Assume that the equation $f(x) = 0$ has one and only one root in an interval (a, b).
Write down the procedure, and mention why *concurrent-read-concurrent-write* option is needed for the memory.
[16]

4. Describe a cost-optimal parallel *selection* algorithm to select the *k-th* element from an input sequence. Specify your model of computation and analyze the time complexity and cost.
[12 + 6 =18]

5. Given two polygons Q and R with m and n edges respectively, $m \leq n$, describe an $O(\log n)$ parallel algorithm to find if Q and R intersect. Show the specific architecture. Assume that the polygons are represented by the edges. Analyze the time complexity and the cost.
[12 + 4=16]

6. a) State whether the following statements are true (T) or false (F):

   i. CUDA splits problems into grids of blocks, each containing multiple threads.

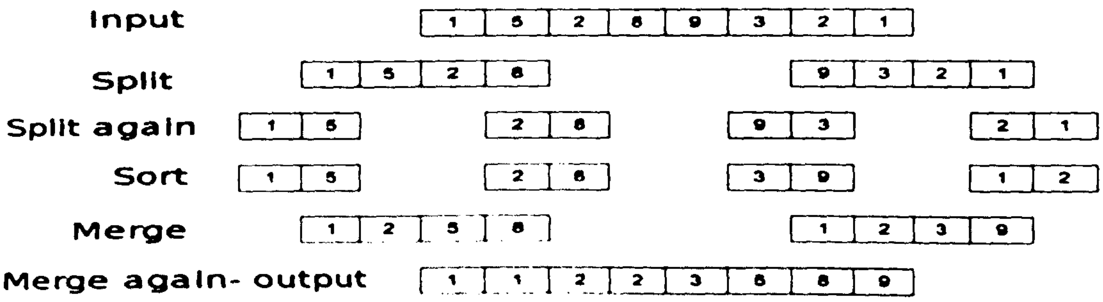
   ii. Blocks are allocated from the grid of blocks to any SM that has free slots.

   iii. *Constant memory* is used when the data does not fit into the *registers*.

   iv. A thread block is an array of threads that can cooperate, synchronize and share data in shared memory.

   v. Warp is a group of threads that always execute same instructions simultaneously.

   b) Write a parallel CUDA kernel code to sort a large input array using the *Merge Sort* technique presented below for sorting 8 elements.



Explain the implementation procedure in brief.

[5+15=20]

INDIAN STATISTICAL INSTITUTE

First Semester Examination 2017-18

M.Tech.(CS) - Second Year

Subject: Pattern Recognition and Image Processing

Date: 29/11/2017 Maximum Marks: 100 Duration: 3 hrs.

Please keep your answers brief and to the point.

Each of the questions carry 20 marks

Answer any five questions

1.

a. In which of the following cases will *k*-means clustering fail to give good results? Explain the reason for your answer. [3x4=12]
   i. Data points with outliers
   ii. Data points with different densities
   iii. Data points with round shapes
   iv. Data points with non-convex shapes

b. What is 'Overfitting' in machine learning? How can you avoid it? [3]

c. What is the "Curse of Dimensionality?" [2]

d. Define **three** class separability measures. [3]

2.

a. What do you mean by image segmentation? [2]

b. Describe a criterion for segmenting an image into *n* sub-regions. [3]

c. What do you mean by convolution operation? [3]

d. Find the convolution of an image *x(m, n)* and a filter *h(p, q)* given below: [8]

0	123	102	11
255	42	111	73
16	89	64	32
27	55	30	0

x(m, n)

2	-1	-1
-1	2	-1
-1	-1	2

h(p, q)

e. Identify what the filter *h(p, q)* will do to an image. [4]

3.

a. What are the assumptions of Otsu's image segmentation method? [2]

b. Describe this optimal thresholding technique. [8]

c. Define Histogram of an image. [2]

d. Equalize the following histogram: [8]

Gray Levels	0	1	2	3	4	5	6	7
Number of pixels	790	1023	850	656	329	245	122	81

4.

a. Show how the string "the brown cow eats grass" is encoded in ASCII. [3]

b. How is Huffman coding used to compress the above string resulting in still more savings? [8]

P.T.O

c. Define filter and wrapper approaches for feature selection. State the differences between them and give some examples. [4+5]

5.

a. Differentiate between similarity measures and proximity measures. Give one examples for each. [4]

b. What is the best distance (or similarity) measure for each of the following applications? Explain why. [4x3=12]

   i. Calculate driving distance between two locations in Kolkata;
   ii. Compare similar diseases with a set of medical test results as positive or negative;
   iii. Find similar web documents to a keyword query.

c. State the essential properties of a distance measure. [4]

6.

a. The table below shows a confusion matrix for a two class classification problem. Calculate the following measures: [2x4=8]

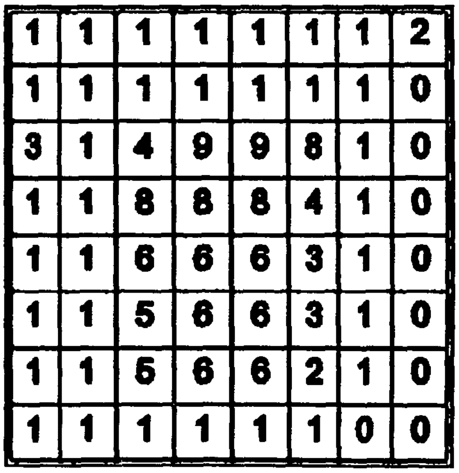
	Predicted +	Predicted -
True +	100	40
True -	60	300

Confusion Matrix

   i. Accuracy,
   ii. Precision,
   iii. Recall,
   iv. *f*-measure.

b. Can you cite **one** example where a false negative is more important than a false positive? [2]

c. Consider the following image and show how the split and merge algorithm will result into distinctly segmented regions. Show each step. [10]



1	1	1	1	1	1	1	2
1	1	1	1	1	1	1	0
3	1	4	9	9	8	1	0
1	1	8	8	8	4	1	0
1	1	6	6	6	3	1	0
1	1	5	6	6	3	1	0
1	1	5	6	6	2	1	0
1	1	1	1	1	1	0	0

Indian Statistical Institute

Semester Examination: 2017 – 2018

Master of Technology in Computer Science, Semester III

Functional Brain Signal Processing: EEG & fMRI (B50)

Date: 1 December 2017 Maximum Marks: 100 Duration: 3 hours

Attempt all the questions. Credit will be given for precise and brief answers.

1. Describe in detail and with diagram, if necessary, how acquisition of T_1 and T_2 imaging are made. Read the following table carefully. Now, decide in case of MR imaging of a brain tumor what should be the minimum TR for a very good quality image and why? Please note that there is no exact answer to this question. Write your reasoning in detail on which evaluation will be made. 5 + 5 + 10 = 20

Tissue	T_1	T_2
Fat	241	85
Brain, white matter	683	90
Brain, gray matter	813	100
CSF	2500	1400

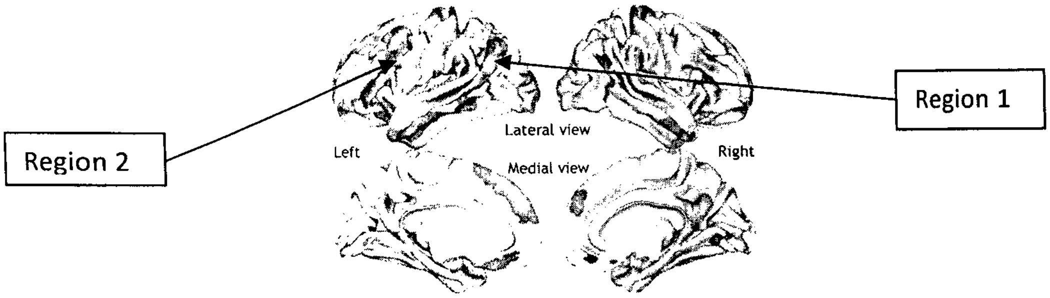
2. What is functional MR imaging? Which among the structural and the functional MR imaging has poorer signal to noise ratio and why? Describe how fMRI depends on four major parameters. 5 + 3 + 3 x 4 = 20

3. (a) Let $\mathbf{M}_{m\times n}$ be an $m\times n$ real matrix. Show that linear spaces generated by columns of $\mathbf{M}_{m\times n}$ and $\mathbf{M}^T_{m\times n}\mathbf{M}_{m\times n}$ are the same. Prove that $\mathbf{M}^T_{m\times n}\mathbf{M}_{m\times n}\mathbf{a} = \mathbf{M}_{m\times n}\mathrm{Y}$ will have a unique solution in $\mathbf{a}$ even if $\mathbf{Y} = \mathbf{Ma}$ does not have a unique solution. $\mathbf{a}$ is an $n\times 1$ variable matrix and $\mathbf{Y}$ is an $n\times 1$ fixed matrix. 4 + 6 = 10

   (b) In General Linear Model (GLM) for fMRI data analysis let individual level model be defined as $\mathbf{Y}_k = \mathbf{M}_k\mathbf{a}_k + \mathbf{e}_k$, where k stands for kth subject, $\mathbf{Y}_k$ is the voxels time series matrix, $\mathbf{M}_k$ is the regressor matrix and $\mathbf{e}_k$ is the additive error signal matrix. With this, formulate the group level GLM problem and show that it has unique solution. 10

4. (a) How an 'active' voxel is identified in an fMR image of the whole brain? 3

(b) Consider the following fMR image of the brain during a particular task performance.



Obviously, multiple voxels are active, some are adjacent to each other and some are far apart. Assuming that different functionally specialized areas of the brain are active simultaneously in order to perform that task, what method(s) will you use for analyzing the time series data of the activation pattern of (1) the adjacent active voxels (for example, within Region 1 in the figure), and (2) between the active voxel clusters far apart (for example, between Region 1 and Region 2 in the figure)? What will be your approach if the number of regions is more than two? There are many different ways this problem can be approached. Evaluation will be done on the logical steps of the approach. Feel free to be imaginative. 5 + 5 + 7 = 17

5. Why simultaneous EEG-fMRI recording is advantageous? Name five significant challenges against getting good quality EEG signals in an MR environment. You will also have to write why they are challenging against the quality of the EEG signals. How cortical source localization of scalp EEG can be improved through simultaneous EEG-fMRI recordings? 2 + 5 x 3 + 3 = 20

INDIAN STATISTICAL INSTITUTE

First Semester Examination: 2017-2018

M. Tech. (CS) II year

Data Mining and Knowledge Discovery

Date: 1.12.2016 **Maximum Marks: 100** **Duration: 3 hours**

1. (i) Enumerate the merits and demerits of hierarchical clustering.
   (iii) Describe algorithm CLARANS.
   (iii) Why do we need density based clustering?
   (iv) What are some drawbacks of DBSCAN? [4+7+4+3=18]

2. (i) What are association rules?
   (ii) Describe the Apriori algorithm.
   (iii) What is cluster validation? [5+8+5=18]

3. Write short notes on any three of the following:
   (i) Generative Adversarial Networks
   (ii) Siamese Neural Networks
   (iii) Graph Mining
   (iv) Long Short Term Memory
   (v) Web Mining [7+7+7=21]

4. (i) In the context of a Multi-Layer Perceptron (MLP) training, explain carefully the relation between Weight Decay and cost function Regularization.

(ii) What is the role of pooling layers in a CNN?

(iii) A convolutional neural network has 4 consecutive 3x3 convolutional layers with stride 1 and no pooling. How large is the support of (the set of image pixels which activate) a neuron in the 4th non-image layer of this network?

(iv) Hinton describes dividing the learning rate for a given weight by a running average of the magnitude of recent gradients for that weights. What is the intuition behind this method? What problems does it help to solve?

(v) Why might one want to add noise to the training data when training a neural network? Should the noise be added to the inputs, the target outputs, or both? Suggest a procedure for determining what level of noise is appropriate.

(vi) Can you provide an example of a common compression system that could be implemented using auto-encoders? [2+3+3+2+4+4=18]

P.T.O

5. (i) Consider a convolution layer. The input consists of 6 feature maps of size 20×20. The output consists of 8 feature maps, and the filters are of size 5 × 5. The convolution is done with a stride of 2 and zero padding, so the output feature maps are of size 10 × 10.

A) Determine the number of weights in this convolution layer.

B) Suppose we made this a fully connected layer, where the number of input and output units are kept the same as in the network described above. Determine the number of weights in this layer.

C) Recall that the learning rate is an example of a hyper-parameter which must be tuned. Alice wants to tune the learning rate by doing a grid search over values and choosing the one which achieves the lowest training error. Bob tells her it's important to tune all hyper-parameters on a separate validation set. Who is right? Justify your answer.

(ii) Design a multilayer perceptron which receives three binary-valued (i.e. 0 or 1) inputs x1, x2, x3, and outputs 1 if exactly two of the inputs are 1, and outputs 0 otherwise. All of the units use a hard threshold activation function:

$$z = \begin{cases} 1 & \text{if } z \geq 0 \\ 0 & \text{if } z < 0 \end{cases}$$

Specify weights and biases which correctly implement this function. Explain your solution.

(Hint: one of the hidden units should activate if 2 or more inputs are on, and the other should activate if all of the inputs are on.)

(iii) Suppose you have a neural network model with an infinite stream of inputs and targets from users surfing the Web. How do you choose its hyper-parameters?

(iv) Compare and contrast (providing specific differences, advantages and disadvantages) the following activation functions: **Hyperbolic tangent (tanh), Rectified Linear Unit (ReLU), Leaky ReLU (LReLU).**

[(3+3+4)+6+3+6=25]

INDIAN STATISTICAL INSTITUTE

First Semester Examination: 2017-2018

M. Tech. (CS) II year

Data Mining and Knowledge Discovery

Date: 1.12.2016 **Maximum Marks: 100** **Duration: 3 hours**

1. (i) Enumerate the merits and demerits of hierarchical clustering.
   (iii) Describe algorithm CLARANS.
   (iii) Why do we need density based clustering?
   (iv) What are some drawbacks of DBSCAN? [4+7+4+3=18]

2. (i) What are association rules?
   (ii) Describe the Apriori algorithm.
   (iii) What is cluster validation? [5+8+5=18]

3. Write short notes on any three of the following:
   (i) Generative Adversarial Networks
   (ii) Siamese Neural Networks
   (iii) Graph Mining
   (iv) Long Short Term Memory
   (v) Web Mining [7+7+7=21]

4. (i) In the context of a Multi-Layer Perceptron (MLP) training, explain carefully the relation between Weight Decay and cost function Regularization.

(ii) What is the role of pooling layers in a CNN?

(iii) A convolutional neural network has 4 consecutive 3x3 convolutional layers with stride 1 and no pooling. How large is the support of (the set of image pixels which activate) a neuron in the 4th non-image layer of this network?

(iv) Hinton describes dividing the learning rate for a given weight by a running average of the magnitude of recent gradients for that weights. What is the intuition behind this method? What problems does it help to solve?

(v) Why might one want to add noise to the training data when training a neural network? Should the noise be added to the inputs, the target outputs, or both? Suggest a procedure for determining what level of noise is appropriate.

(vi) Can you provide an example of a common compression system that could be implemented using auto-encoders? [2+3+3+2+4+4=18]

P.T.O

5. (i) Consider a convolution layer. The input consists of 6 feature maps of size 20×20. The output consists of 8 feature maps, and the filters are of size 5 × 5. The convolution is done with a stride of 2 and zero padding, so the output feature maps are of size 10 × 10.

   A) Determine the number of weights in this convolution layer.

   B) Suppose we made this a fully connected layer, where the number of input and output units are kept the same as in the network described above. Determine the number of weights in this layer.

   C) Recall that the learning rate is an example of a hyper-parameter which must be tuned. Alice wants to tune the learning rate by doing a grid search over values and choosing the one which achieves the lowest training error. Bob tells her it's important to tune all hyper-parameters on a separate validation set. Who is right? Justify your answer.

(ii) Design a multilayer perceptron which receives three binary-valued (i.e. 0 or 1) inputs x1, x2, x3, and outputs 1 if exactly two of the inputs are 1, and outputs 0 otherwise. All of the units use a hard threshold activation function:

$$z = \begin{cases} 1 & \text{if } z \geq 0 \\ 0 & \text{if } z < 0 \end{cases}$$

Specify weights and biases which correctly implement this function. Explain your solution.

(Hint: one of the hidden units should activate if 2 or more inputs are on, and the other should activate if all of the inputs are on.)

(iii) Suppose you have a neural network model with an infinite stream of inputs and targets from users surfing the Web. How do you choose its hyper-parameters?

(iv) Compare and contrast (providing specific differences, advantages and disadvantages) the following activation functions: **Hyperbolic tangent (tanh), Rectified Linear Unit (ReLU), Leaky ReLU (LReLU).**

[(3+3+4)+6+3+6=25]

INDIAN STATISTICAL INSTITUTE

End-Semestral Examination: 2017

Date : 04.12.2017

Subject Name : **Cryptology**

Course Name : M.Tech. (CS) II yr. Max Score: 60 Duration: 180 Mins

Note: Attempt all questions. Marks are given in brackets. Total score is 70. But maximum you can score is 60. Use separate page for each question.

1.[4 + 4 +4 = 12] State RSA signature scheme and show its correctness. Define universal forgery security. Is RSA signature secure under universal forgery attack? Justify.

2.[4+4=8] Describe any hybrid signcryption algorithm for a long message. You must show the correctness of your signcryption algorithm.

3.[4 + 8 =12] Let $pad(m_1, \ldots, m_r) = (m_1, \ldots, m_r, \oplus_{i=1}^{r} m_i)$. Show that it is not a prefix-free padding. Construct a forgery attack on $SIV(Mac, Ctr)$ where the Mac is the CBC-MAC with the above padding rule.

4.[2 + 6 = 8] Describe ideal random permutation. Show that message recovery is hard for an ideal random permutation.

5.[10] Let $f, g : \{0,1\}^{n+b} \rightarrow \{0,1\}^n$ be compression functions. Describe a method to construct 4 multicollision set for the hash function $MD^f||MD^g$ in $O(2^{n/2})$ complexity.

6.[8] Let E_K be an n-bit blockcipher with k bit key. We define a compression function $f : \{0,1\}^{k+2n} \rightarrow \{0,1\}^n$ as $f(h, m, m') = (E_h(m) \oplus m) \oplus (E_h(m') \oplus m')$. Construct a collision attack on f in $O(1)$ time.

7.[4 + 8 =12] For an n-bit function (unkeyed) p we define $E_K(x) = p(K \oplus x) \oplus K$ where $K, x \in \{0,1\}^n$. State all conditions for which E will be considered as blockcipher. Find a key recovery attack of the blockcipher in $O(2^{n/2})$ complexity.

Indian Statistical Institute
Mid-Semester Examination (2018)
M.Tech.(CS) II Year
Computer Vision

Date: 20.02.2018 **Full Marks: 60** **Duration – 2 hours 30 mins**

Answer as many questions as you like, but you can at most score 60.

1. (a) Explain clearly what is meant by world co-ordinate and camera co-ordinate respectively. (b) What is the basic task of computer vision with respect to these co-ordinate systems? (c) Is the same task applicable in biological vision too? Explain your answer. (d) Prove that the world point cannot be uniquely determined from the camera co-ordinates by applying inverse perspective transformation in a computer vision system. 4+3+3+6=16

2. (a) Derive geometrically the pair of perspective projection equations in the light of a pinhole camera model. Hence explain why distant objects appear smaller and why the parallel railway tracks appear to converge in such a vision system. (b) What happens to the image when the pinhole size in such camera is (i) increased and (ii) decreased (c) The focal length of a pinhole camera is 10 mm. A scene point is located at (X, Y, Z) = (4m, 8m, 10m). Calculate the corresponding image plane co-ordinates for this scene point. If the dimension of the image plane is 20 mm x 20 mm, what should be the field of view for this pinhole camera? How far away does one have to be with the pinhole camera from a building that is 200 m wide so that its entire field of view is utilized? (4+2+3)+(2+3)+(3+3+4)=24

3. (a)What is a shift invariant linear system in the context of signal processing? How can you explain linear image transforms in this light? (b)Is Gaussian filtering of an image a linear transformation? Hence state what are the advantages of Gaussian filtering for which it is frequently used in computer vision. (c) What is the significance of using such operators in vision that combine different orders of derivative with Gaussian filtering? 4+5+5=14

4. Write short notes on the following: (a)Helmholtz reciprocity condition (b) Lambertian and specular surface (c) radiance and irradiance 4+4+4=12

INDIAN STATISTICAL INSTITUTE

MIDTERM EXAMINATION
M.TECH(CS) II YEAR

ADVANCED CRYPTOLOGY

Date: 20.02.2018 Maximum marks: 60 Duration: 2.5 hours.

The paper contains 72 marks. Answer as much as you can, the maximum you can score is 60.

1. (a) Define a weak one way function.

   (b) Prove that if f is a strong one-way function then $g(x_1, x_2) = (f(x_1), x_2)$, where $|x_1| = |x_2|$, is also a one-way function.

   (c) Let f be a strong one-way function. For a probabilistic polynomial time algorithm $\mathcal{A}$ and a polynomial p, define

   $$B_{\mathcal{A},p} = \left\{x : \Pr\left[\mathcal{A}(f(x)) \in f^{-1}(f(x))\right] \geq \frac{1}{p(|x|)}\right\}.$$

   Prove that for every polynomials p, q, every probabilistic polynomial time algorithm $\mathcal{A}$ and sufficiently large n,

   $$\frac{|B_{\mathcal{A},p} \cap \{0,1\}^n|}{2^n} < \frac{1}{q(n)}.$$

   [4+8+12 = 24]

2. (a) Define hardcore predicate for a one-way function.

   (b) Let $f : \{0,1\}^* \to \{0,1\}^*$ be a strong one-way function. Define $h : \{0,1\}^* \to \{0,1\}$ as $h(x) = \oplus_i x_i$, i.e., $h(x)$ is the xor of all the bits of x. Justify whether $h(x)$ is a hardcore predicate for f.

   (c) Describe the Rabin collection of functions.

   (d) Prove that if factorization assumption holds then Rabin is a one way collection.

   [4+6+2+12= 24]

3. (a) Define the following: (a) Pseudorandom Ensemble (b) Unpredictable ensemble.

   (b) Prove that an ensemble $\{X_n\}_{n\in\mathbb{N}}$, where X_n takes values in $\{0,1\}^n$, is unpredictable if and only if it is pseudo-random.

   [6+18= 24]

INDIAN STATISTICAL INSTITUTE

Periodical Examination

M. Tech (CS) - II Year (Semester - II)

Topics in Algorithm and Complexity

Date : 20.2.2018 Maximum Marks : 60 Duration : 3 Hours

1. Consider the following incremental algorithm for computing the convex hull of a set P of n points in $I\!R^2$.

```
Step 1:   Permute the points in $P$ randomly.
Step 2:   Let $H = CONV(p_0, p_1, p_2)$ be the initial convex hull.
Step 3:   For $i = 3, 4, \ldots, n-1$ do
Step 3.1:     If $p_i \notin H$ then $H = CONV(H, p_i)$
Step 4:   Report $H$
```

   Explain the method along with the necessary data structure for

   (a) testing whether $p_i \notin H$, and

   (b) implementing the statement $H = CONV(H, p_i)$.

   State the worst case time complexity of your proposed method.
   Also, show that this can be implemented in a manner such that the expected time complexity is $O(n \log n)$.
   Justify that the expected time complexity of computing convex hull of a point set can not be improved beyond $O(n \log n)$. [(3+3+3+2)+5+4=20]

2. Propose a randomized polynomial expected running time algorithm for finding the truth assignment of the variables of a MAX-3-SAT problem that satisfies at least $\frac{7}{8}k$ clauses, where k is the number of clauses in the given 3-SAT formula. [10]

3. Suppose you are given a set P of n points, and a constant δ. Write a method for testing whether the distance between the closest pair of points is less than δ in $O(n)$ time.

   Use this method to propose an algorithm for finding the closest pair in expected $O(n)$ time. [7+8=15]

4. Consider a set system with the set of elements S with n elements, and a set of subsets $S_i, i = 1, 2, \ldots, m$, where each $S_i \subseteq S$. The objective is to color the elements in S using "RED" and "BLUE" such that the discripancy $D = \max_{i=1}^{m} [|R_i| - |B_i|]$ is minimized, where R_i (resp. B_i) = set of elements in S_i that are colored "RED" (resp "BLUE").

   Show that, if you color the elements of S by the two said colors with equal probability, then $Probability[D \leq \sqrt{12n \log m}] \geq 1 - \frac{1}{m}$. [10]

5. Given a k-SAT formula,

   (a) show that if no variable of that SAT formula occurs in more than $\frac{2^{k-2}}{k}$ clauses, then it always have a satisfying assignment.

   (b) Also show that such an assignment can be obtained in polynomial time with high probability.

[5+10=15]

INDIAN STATISTICAL INSTITUTE

Mid Semester Examination: (2017-2018)

M. Tech. (CS) – II Yr.

Advanced Pattern Recognition

Date: 22.02.2018 Maximum marks: 50 Duration: 2 hrs

Answer as many questions as you can. Maximum you can score is 50.

1. (a) Suppose two classes have probability distribution functions $f_1(x)$ and $f_2(x)$ with prior probabilities P_1 and P_2 respectively where $0 < P_1, P_2 < 1$ and x represents a *p*-dimensional vector. Define the optimal Bayes boundary for classification for the two classes and write down the expression for the corresponding misclassification probability.

   (b) Suppose two classes have bivariate normal distributions with mean vectors $(0,0)^T$ and $(2,2)^T$ and a common covariance matrix $\sum = \begin{pmatrix} 4 & -1 \\ -1 & 4 \end{pmatrix}$

   The two classes have the same prior probabilities. Derive the optimal Bayes boundary for classification that gives the minimum misclassification probability. Show that this boundary is linear.

   [5 + 12 = 17]

2. (a) Define the first principal component of a multivariate distribution.

   (b) Let $X=(X_1, X_2)^T$ be a random vector that takes the following 5 values with equal probabilities: $(3, 4)^T$, $(4, 3)^T$, $(0, 0)^T$, $(-3, -4)^T$, $(-4, -3)^T$. Find the first principal component of X. Justify your answer.

   [3 + 10 = 13]

3. Write brief answers.
   a) What is the difference between the perceptron learning rule and the delta rule?
   b) Deduce what happens to the derivative of the sigmoid function $f(x)$ when $x = 1$.
   c) What is the role of gradient descent in the delta rule?
   d) Give a simple example of a set of input-output patterns that cannot be represented by a perceptron network of input and output units without any arrangement for internal representation.
   e) State two ways of reducing the number of presentations of input samples to a multilayer perceptron with backpropagation learning algorithm to reach the solution and their possible drawbacks.

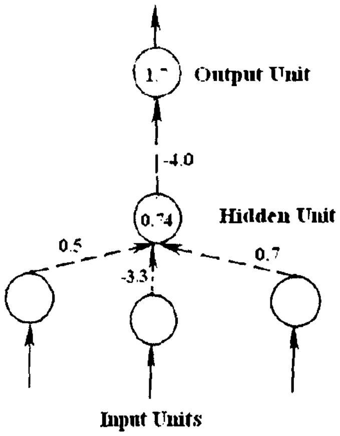
   [2 + 2 + 2 + 2 + 2 = 10]

[Please turn over]

4. Consider the following set of input-output patterns and the attached network architecture. Find the patterns that are correctly classified by the network.

Input			Output
1	0	0	0
0	1	0	1
0	0	1	0
1	1	0	1

Connection weights are shown alongside the arrows and the thresholds are written inside the circles.



[5]

5. Given a set of k samples $\{(x_i, y_i);\ i = 1, 2, \ldots, k\}$, where $x_i \in R^n$ and $y_i \in \{0, 1\}$ of two categories, use the method Linear Discriminant Analysis to obtain the classification rule.

[5]

6. Consider the following two sets S_1 and S_2 of 2-dimensional samples from two classes C_1 and C_2 respectively. Use the method of Fisher's Linear Discriminant Analysis to obtain the projected samples down to one dimension.
$S_1 = \{(4,1), (3,1), (6,2), (4,3)\}$ and $S_2 = \{(6,6), (3,9), (4,8), (6,10)\}$

[10]

Indian Statistical Institute
Semester-2 2017-2018
M.Tech.(CS) - Second Year
Mid-semester Examination (22 February, 2018)
Subject: Compiler Construction
Total: 35 marks Maximum marks: 30 Duration: 2 hrs.

Please keep your answers brief and to the point.

1. Consider a file that contains some English text. Each word is a sequence of lowercase / uppercase letters; no digits occur in the file. Words are separated by whitespace (blanks / tabs / newlines) or punctuation (., !, ?, ,, ;, :, (, and)). Paragraphs are separated by one or more lines containing whitespace only. Write a Lex program that takes such a file as input, and prints the same text as output, such that

   - individual words within a paragraph are separated by a **single** blank space if no punctuation mark appears between the two words;
   - paragraphs start with two blank spaces, and end with a newline character;
   - any two paragraphs are separated by a **single empty line**;
   - any punctuation mark except '(' occurs immediately after the preceding word, and is followed by a **single** blank;
   - the open parenthesis is preceded by a single blank (unless it occurs at the start of a paragraph), and is immediately followed by the next word.

   You may make reasonable additional assumptions if necessary. **Clearly state your assumptions.**

   [12]

2. Consider the following grammar (assume that any symbol that does not have an associated production rule is a terminal):

$$S \rightarrow S : S \qquad S \rightarrow id = E \qquad S \rightarrow \text{print}(L)$$
$$E \rightarrow E + T \qquad E \rightarrow E(E) \qquad E \rightarrow T \qquad T \rightarrow id$$
$$L \rightarrow E \qquad L \rightarrow L, E$$

   (a) Eliminate left-recursion from the given grammar and do left factoring if necessary.

   (b) Compute the *FIRST* set for the right hand side of each rule of the modified grammar.

   (c) Compute the *FOLLOW* set for each non-terminal of the modified grammar.

   (d) Construct the $LL(1)$ parsing table for the modified grammar.

   (e) Show that the original grammar is ambiguous.

   (f) Modify the grammar so that it generates the same language but is unambiguous.

   [4 + 3.5 + 6 + 4.5 + 2 + 3 = 23]

INDIAN STATISTICAL INSTITUTE
Mid-Semester Examination
M. Tech. (CS) II year (2nd Sem): 2017–2018
Logic for Computer Science

Date: 22. 02. 2018 Total Marks : 72 Time : 2.5 Hours

Answer as much as you can. Maximum you can score is 60.

1. (a) Explain Cantor's paradox.

   (b) Express the XOR operator in terms of the IMPLICATION and the NOT operators.

   (c) What is the difference between *Truth* and *Tautology*?

   [4 + 4 + 4]

2. What is a *logical theory*? What is meant by *completeness* and *soundness* of a logical theory? [4 + 4 + 4]

3. (a) How many axioms are there in the classnote version of *Propositional Logic* (PL)?

   (b) What is an *axiom-schema*?

   (c) Are the following problems of PL decidable?

      i. Whether an expression is a *well-formed formula* (wff)?

      ii. Whether a wff is an axiom?

      iii. Whether a wff is a theorem?

      iv. Whether a wff is provable?

      v. Whether a wff is satisfiable?

   [2 + 4 + (2 + 2 + 2 + 2)]

4. Consider the following 5 definitions.

   (a) A *literal* is an atomic sentence or its negation.

   (b) A *clausal sentence* is either a literal or a disjunction of literals.

   (c) A *clause* is the set of literals in a clausal sentence.

   (d) Given a clause containing a literal and another clause containing the negation of the same literal, we can infer the clause consisting of all the literals of both the clauses without the complementary pair. This rule of inference is called *Propositional Resolution* or the *Resolution Principle.*

   (e) A *Resolution Proof* of a sentence $\mathcal{A}$ from a set Δ of sentences is derivation of the empty clause from the clausal form of $\Delta \bigcup \neg\{\mathcal{A}\}$.

   Now prove that *Modus Ponens* is a special case of the *Resolution Principle.* Also prove that *Propositional Logic with Resolution Proof* is complete. [4 + 8]

5. Prove the following theorems of PL.

   (a) $(\mathcal{A} \implies \mathcal{B}) \implies ((\neg\mathcal{A} \implies \mathcal{B}) \implies \mathcal{B})$

   (b) $\mathcal{A} \vee \mathcal{B} \implies \mathcal{B} \vee \mathcal{A}$

   (c) $\mathcal{A} \implies (\mathcal{B} \implies (\mathcal{A} \wedge \mathcal{B}))$

   [8 + 6 + 8]

INDIAN STATISTICAL INSTITUTE

Mid-Semester Examination: (2017-2018)
M.Tech C.S., 2nd Year

Advanced Digital Signal Processing

Date: 23.2.2018 Maximum Marks: 60 Duration: 2 hours

Note: The exam is open book and open notes. The marks add up to 78. The maximum you can score is 60.

Questions:

1. Consider a signal

$$x[n] = sin(\pi n/4 + 0.8sin(\pi n/8) + 0.2cos(\pi n/6)$$

How many spectral peaks would be obtained using a 128 point DFT with a 128-point Hamming window? Justify your answer. Suggest how it would be possible to resolve all 3 components. [6+4]

2. Develop a lattice-ladder realization of

$$H(z) = \frac{2.2 + 3z^{-1} + z^{-2}}{1 + 0.2z^{-1} + 0.6z^{-2}}$$

[10]

3. Consider a signal

$$x[n] = \begin{cases} \cos(2\pi n/32) + 0.5\sin(2\pi n/16) & \text{if } 0 \leq n \leq 127 \\ 0 & \text{otherwise} \end{cases}$$

Let the N-point Discrete Fourier Transform (DFT) of $x[n]$ be denoted by $X[k]$, $k = 0, \cdots, N-1$. Sketch $|X[k]|$ for

(a) N = 128.

(b) N = 32.

[5+5]

P.T.O

4. Determine the Short Time Fourier Transform (STFT) using a rectangular window of size 20 and a sampling interval of 10, for the following signal

$$x[n] = \begin{cases} \cos(2\pi n/5) & \text{if } 0 \le n \le 19 \\ \cos(2\pi n/4) & \text{if } 20 \le n \le 39 \\ 0 & \text{otherwise} \end{cases}$$

[10]

5. Consider a white noise sequence with variance 1 and mean 10. Determine the mean and autocorrelation of its N-point DFT sequence. [10]

6. The autocorrelation sequence of an AR process is

$$\gamma_{xx}[m] = (0.5)^m \cos(\pi m/2)$$

   (a) Determine the coefficients of a second order linear predictor for this process.

   (b) If this process is now contaminated by the addition of zero mean white noise with variance 1, determine the coefficients of a second order IIR Wiener Filter and the corresponding MMSE.

[7+7+4]

7. A white-noise sequence $w[n]$ with mean zero and power spectral density 0.5 passes through an LTI system to produce

$$y(n) = 0.6y(n-1) + w(n) + w(n-1)$$

Determine the autocorrelation sequence and power spectral density of the output. [5+5]

Indian Statistical Institute

M.Tech (CS) II

Information Security and Assurance

Mid Semester Examination

Marks:50

Date: February 23, 2018
Time 2 hours

The question paper contains 6 questions. Total marks is 60. Maximum you can score is 50.

1. How can you construct Schnorr Signature scheme using Schnorr identification scheme? Discuss the security of Schnorr Signature scheme. (8+4=12)
2. Currently Certificate Transparency does not handle revoked certificates. Design a data structure and a modified Certificate Transparency protocol to handle revoked certificates. (10)
3. How can Bloom filters be used to construct password checker? Can you suggest an alternate technique. (6+2=8)
4. Can you construct a commitment scheme from (a) an Encryption scheme (b) a Signature Scheme? How is Pedersen commitment scheme different from El Gamal Encryption algorithm? (6+6=12)
5. Prove that if one-way permutations exist, then every language in NP has a zero-knowledge proof. (12)
6. What are kernel mode rootkits, describe one attack by kernel mode rootkits. (2+4=6)

Indian Statistical Institute
Second Semester Examination (2017-18)
M.Tech (CS) II Year
Computer Vision

Date: 16.04.18 **Duration – 3 hours 15 minutes**

Answer as many questions as you like but the maximum you can score is 100

1. (a) Evaluate the Fourier transform g(ω) of a normalized one-dimensional Gaussian function G(x). Plot neatly G(x) vs. x and g(ω) vs. ω.

   (b) Evaluate $G_1(x)$ and $G_2(x)$ where these represent the first and second order derivatives of G(x) respectively and then plot $G_1(x)$ vs. x and $G_2(x)$ vs. x.

   (c) Evaluate and plot the outputs of convolution of a one-dimensional step function with both $G_1(x)$ and $G_2(x)$.

   (d) Explain the significance of each of the results obtained in (a), (b), and (c) in computer vision.

   (6+1+2)+(2+3+1+1)+2 x (3+1)+(2 x 3)=30

2. (a) Explain with neat diagram/s the concept of perspective projection in the light of the pin-hole camera model.

   (b) If f is the focal length of the camera in (a), explain with diagram what do you mean by field of view of the camera.

   (c) Explain briefly how the geometric transformations like Translation, Scaling and Rotation are relevant in the context of camera?

   (d) Derive the transformation matrices for Translation, Scaling and Rotation (consider rotation about Z-axis only) and also their respective inverses.

   4+2+3+(4+4+5)=22

3. (a)What are Purkinje shift and CIE function in colour vision?

   (b) Define photopic response V(λ). You have a 10 mW green laser pointer operating at wavelength 530 nm. Your friend has a red laser pointer, also of power 10mW, operating at wavelength 640 nm. If the values of V(λ) for red and green are 0.1 and 0.9 respectively, can you claim that your green laser pointer will appear much brighter than the red laser pointer of your friend? If yes, state how many times brighter, justifying your answer.

.......contd. to page 2

(c) In the context of radiance-irradiance of a scene, explain diagrammatically the Hemisphere of Directions and foreshortening.

(d) Hence prove that radiance varies directly with irradiance.

(e)Who developed the Retinex theory in computer vision and what are the basic assumptions of this theory?

(f)Explain how the inverse problem of lightness recovery is computationally solved in the light of the Retinex theory.

(2+2)+(2+1+4)+(3+2)+8+(1+2)+5=32

4. Let us consider 2 cameras (Left & Right) with focal lengths f each, a scene point (X, Y, Z), and the corresponding image points on the left camera and right camera P_L (x_L, y_L) and P_R (x_R, y_R) respectively. The Left and Right cameras are separated by a distance δx along the x-axis where all the positions and distances mentioned above are measured from the origin of the left-hand camera's co-ordinate system only. What will be the two sets of perspective transformation equations for the Left and Right cameras? Hence prove that the depth of the scene point is given by:

$$Z = f[1+ \delta x/\{ x_L - (x_R + \delta x)\}]$$

2+4+4=10

5. Write short notes on any two:
   (a) Otsu algorithm
   (b) Gaussian and Laplacian pyramids
   (c) Motion field
   (d) Edge linking

2 x10=20

INDIAN STATISTICAL INSTITUTE

Semester Examination: (2017-2018)

M. Tech. (CS) – II Yr.

Advanced Pattern Recognition

Date: 20.04.2018 Maximum marks: 100 Duration: 3 hrs

Answer as many questions as you can.

1. Consider the task of segmenting a gray level image into the foreground and the background. Assume that the background is lighter than the foreground. Also assume that the gray level values in the image are unlabelled and are random samples from a mixture of normal distributions.

(i) Define such a mixture distribution for the task above clearly indicating all model parameters.

(ii) Provide an algorithm to estimate these parameters on the basis of the unlabelled gray level values in the image.

(iii) Explain how a pixel is classified into the foreground and the background on the basis these estimates. [3+11+3=17]

2. (a) Let f be a positive real valued function defined on the interval [0,7]. Suppose the maximum value of f occurs only at 5. Suppose you have only the crossover operation in a Genetic Algorithm framework with the probability of crossover being $0 < p_c < 1$. If the string length of the chromosome is 3 and the initial population is {000, 111}, then

(i) what is the probability that the maximum value of f will be attained in the first generation after the initial population ?

(ii) what is the probability that the maximum value of f will be attained in the second generation ?

(b) Suppose you have an initial population of chromosomes (*010000, 000111*), and the crossover and mutation probabilities are p_c and p_m respectively. What is the probability that after one round of crossover and mutation stages, the population becomes (*00000, 000111*) ? [(2+7)+11=20]

3. Provide the set of parameters that define a hidden Markov model. Describe an algorithm to compute the probability of a finite sequence (of length T) of observation vectors for a given hidden Markov model with computational complexity not higher than $O\,(Tn^2)$, where n is the number of states. [5+9=14]

4. Define a self organizing neural network and write down the update rules of its weight vectors. Provide the conditions under which the weight vectors converge. [7+4=11]

P.T.O

5. Suppose two classes have univariate probability distribution functions $f_1(x)$ and $f_2(x)$ with equal prior probabilities, where f_1 and f_2 are uniform distributions over (0, 1.1) and (0.9, 2) respectively. Provide an optimal Bayes boundary for classification and justify your answer. Is the boundary unique ? Justify your answer. [4+2=6]

6. (a) What is the purpose of feature selection? What are the two broad categories of approaches to feature selection? What are their merits and demerits?

(b) Name two evaluation criteria used for feature selection. Define F-statistic for one-way-analysis-of-variance. Discuss whether the use of F-statistic is an effective approach towards feature selection.

(c) Write down the mathematical expression of mutual information between two random variables? Discuss its role in feature selection. [(1+2+2)+(2+2+1)+(2+3) = 15]

7. (a) What is the possible difficulty in using a fully connected feed forward multilayer perceptron network for image recognition from raw pixel values? How the connection scheme of such feed forward network architecture can be modified to overcome the difficulty?

(b) What is a feature map? How is the reduced precision feature extraction achieved in such a network? Why is low precise coding for the location of higher-level features required?

(c) Consider a partially connected feed forward network architecture input, which has the dimension 28 × 28. Its first convolution layer C1 has 4 independent feature maps each of which is computed from the input image using a distinct 5 × 5 kernel at each pixel position of the input image barring the 4 boundaries of width 2 each. The next layer S2 implements mean pooling on C1 over non-overlapping 2 × 2 windows. The next convolution layer C3 has another set of 12 independent feature maps. The input receptive field of each unit of a feature map of C3 consists of similar 5 × 5 kernel as in the case of first convolution layer but spanning over all the sub-sampled feature maps of S2. Another layer S4 is used for implementing similar mean pooling on the units of feature maps of C3 as in the case of S2. All the units of S4 are fully connected to a hidden layer H5 of 30 units. H5 is fully connected to the output layer consisting of 10 units. Here, it may be noted that all the units in a feature map share the same set of weights and bias but different feature maps have different sets of weights and biases. Compute (i) the size of each feature map of layers C1, S2, C3 and S4, (ii) the number of connections between input layer and C1, (iii) the number of connections between S2 and C3, (iv) the number of connections between S4 and H5. [(1+1) + (1+1+1) + (4×1 + 4 + 4 +1) = 18]

8. (a) Obtain Fisher's linear discriminant function for two classes based on a training set.

(b) Write down the backpropagation part of the backpropagation algorithm to train a multiplayer perceptron containing only one hidden layer. Mention the dimensions of various weight matrices. [Here, assume X, Y and Z respectively denote input, target and output vectors of dimensions *n*, *m* and *m* respectively.]

(c) Describe the kernel trick used in Support Vector Machines. [8 + 4 + 4 = 16]

Indian Statistical Institute

Semester-2 2017-2018

M.Tech.(CS) - Second Year

End-semester Examination (20 April, 2018)

Subject: Compiler Construction

Total marks: 65 Maximum marks: 60 Duration 3.5 hrs.

Please keep your answers brief and to the point.

1. Consider the following grammar (capital letters denote non-terminals, small letters denote terminals):

$S \rightarrow Aa \mid bAc \mid Bc \mid bBa$
$A \rightarrow d$
$B \rightarrow d$

(a) Construct the canonical collection of LR(1) items for this grammar. You should get about 13 sets in the collection.

(b) **Without constructing the complete parsing table**, argue why this grammar is LR(1), but not LALR. [6 + 3 = 9]

2. Consider the following syntax-directed definition (SDD):

```
L -> id [ Elist ]      { Elist.array = lookup(id.name); Elist.ndim = 1;
                         L.place = Elist.array;
                         L.offset = Elist.place * elt_size(Elist.array); }
Elist -> Elist1 , E    { Elist1.array = Elist.array; Elist1.ndim = Elist.ndim+1; }
                         Elist.place = E.place +
                             Elist1.place * num_elts(Elist1.array, Elist1.ndim); }
Elist -> E             { Elist.place = E.place; }
```

(a) Explain in 1 line each whether Elist.array, Elist.ndim, Elist.place, L.place, L.offset, are inherited or synthesized attributes.

(b) Convert the SDD into an equivalent translation scheme (TS) by embedding actions at appropriate places in the RHS of each rule.

(c) Convert the TS into a form suitable for bottom-up parsing by using markers.

(d) Re-write the semantic actions in your TS in terms of elements of the value stack. (Assume that attributes are stored in the usual positions in the value stack during bottom-up parsing.)

[2.5 + 2.5 + 1 + 8 = 14]

3. (a) Using a grammar like the one discussed in the textbook/class, draw the parse tree for the following code fragment:

```
while (i < N && flag != 0 || j > 0) do i = j + 1;
```

(b) Use backpatching to generate 3-address code for the above. Annotate the relevant nodes in your parse tree with the lists maintained by the backpatching algorithm.

[3 + (3 + 4) = 10]

P.T.O

4. A two-dimensional array A is said to be stored in *column major* form if its elements are stored in memory in the following sequence:

$A[0,0]\ A[1,0]\ A[2,0]\ \ldots\ A[n_1-1,0]\ A[0,1]\ A[1,1]\ \ldots A[n_1-1,1]\ \ldots A[0,n_2-1] \ldots A[n_1-1,n_2-1]$

In general, in column major storage, the elements of a multi-dimensional array are stored such that when they are traversed in order, the left-most index varies most rapidly and the right-most index varies the slowest.

For a particular element $A[i_1, i_2, \ldots, i_m]$ of an m-dimensional array $A[n_1, n_2, \ldots, n_m]$, let e_m be the number of elements stored in memory before the given element. Show that

$$\begin{aligned} e_1 &= i_1 \\ e_2 &= i_1 + i_2 \times n_1 \\ e_3 &= i_1 + i_2 \times n_1 + i_3 \times n_1 \times n_2 \end{aligned}$$

Hence argue that

$$e_m = e_{m-1} + i_m \times \prod_{j=1}^{m-1} n_j$$

[7]

5. Consider the following procedure in C.

```
void transpose(int A[20][10])
{  int i, j;
   for (i=0; i < 20; i++)
       for (j = i+1; j < 10; j++) {
           t = A[i][j]; A[i][j] = A[j][i]; A[j][i] = t;
       }
}
```

(a) Convert the body of the procedure into 3-address code. Each time a temporary variable is needed, use a new temporary. You may use the name of an array instead of the constant (base address) associated with that array. **Do not perform any optimization at this stage.**

(b) Assume that arrays like A are passed by reference (not by value). Also assume that integers, pointers and temporaries each occupy 4 bytes, and that it takes 128 bytes to store the saved machine status. Draw a suitable layout for the Activation Record (AR) for transpose (including byte offsets).

(c) Write the machine code for the calling sequence and return sequence for a call to transpose from main. Assume that (i) the stack grows from low addresses to high addresses; (ii) the stack pointer points to the beginning (i.e. lowest address) of an AR; and (iii) the AR for main occupies 320 bytes.

(d) Identify the leaders (and thus the basic blocks) in the 3-address code in (a). Draw the flow-graph for this code.

(e) Optimize your intermediate code by using whichever of the following techniques are applicable: constant folding, global common sub-expression elimination, copy propagation, dead code elimination, code motion, induction variable elimination.

[You do not have to show the intermediate code after each stage of optimisation. You may simply write down the final optimised code.]

[7 + 3 + 4 + (3 + 3) + 5 = 25]

INDIAN STATISTICAL INSTITUTE

Second Semester Examination: 2017-18

M.TECH(CS) II YEAR

ADVANCED CRYPTOLOGY

Date: 20.04.2018 Maximum marks: 100 Duration: 3.5 hours.

The paper contains 110 marks. Answer as much as you can, the maximum you can score is 100.

1. (a) Define a weak one-way function.

   (b) Let f be an injective function with a hard-core predicate b. Show that if f is polynomial time computable then f is strongly one-way.

   (c) Given a pseudorandom generator G which expands n bit inputs to $2n$ bits, construct a pseudorandom function ensemble $F = \{F_n\}_{n \in \mathbb{N}}$ using G. No proof required.

   (d) Let $\{F_K\}_{K \in \mathcal{K}}$ be a pseudorandom function family where for each $K \in \mathcal{K}$, $F_K : \{0,1\}^n \rightarrow \{0,1\}^n$. Define another family $\{G_K\}_{K \in \mathcal{K}}$, where for each $K \in \mathcal{K}$, $G_K : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ is defined as $G_K(x) = F_K(x)||F_K(F_K(x))$. Is $\{G_K\}_{K \in \mathcal{K}}$ a pseudorandom family? Justify.

   $[4 + 8 + 6 + 4 = 22]$

2. (a) Derive the sum and doubling formulae for points in an an elliptic curve $E : y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_p$, and $4a^3 + 27b^2 \neq 0$.

   (b) For points $P, Q \in E(\mathbb{F}_p)$, let $\mathsf{sum}(P, Q)$ and $\mathsf{dbl}(P)$ be procedures for computing $P + Q$ and $P + P$ respectively. For a given point $X \in E(\mathbb{F}_p)$ and $a \in \mathbb{Z}^+$ write an efficient algorithm using $\mathsf{sum}(.,.)$ and $\mathsf{dbl}(.)$ to compute aX. Appropriate checks should be put so that the algorithm runs for all cases.

   (c) Let $E/\mathbb{F}_p$ be the elliptic curve $y^2 = x^3 + ax + b$ and let $P \neq \infty$ be a point in $E(\mathbb{F}_p)$. We denote the x-cordinate of point P by $x(P)$. For an integer $\alpha \neq 0$, let $x_\alpha = x(\alpha P)$ when $\alpha P \neq \infty$. Using the addition formulae derived in Question 2(a), derive formulae for $x_{2\alpha}$ and $x_{2\alpha+1}$ which involves only x_α, $x_{\alpha+1}$, x_1, a and b. State clearly the cases where your derived formulae does not work.

   (d) Use the formulae derived in Question 2(c) to devise an algorithm to compute x_α from x_1. Your algorithm should take $\lceil \lg \alpha \rceil$ steps.

   $[12 + 10 + 10 + 12 = 44]$

3. (a) Define a symmetric admissible bilinear pairing.

   (b) Describe a one-round tripartite key-exchange scheme.

   (c) Let $\mathcal{G}$ be a BDH instance generator, i.e., $\mathcal{G}$ on input a security parameter k outputs (q, G_1, G_2, e, P) where q is a prime, G_1, G_2 are (descriptions of) groups of order q, $e : G_1 \times G_1 \to G_2$ an admissible symmetric bilinear pairing and P a generator of G_1.

      (i) State the Bilinear Diffie Hellman (BDH) problem with respect to $\mathcal{G}$.

      (ii) Show how the DDH problem in G_1 can be solved given e.

   (d) Let $e : G_1 \times G_1 \to G_2$ be a symmetric admissible bilinear pairing, where both G_1 and G_2 are prime order groups of order q. For a fixed but arbitrary $Q \in G_1^*$ define the isomorphism $f_Q : G_1 \to G_2$ by $f_Q(P) = e(P, Q)$. Show that if the DDH problem is hard in G_2 then f_Q is strongly one-way.

[$3 + 3 + (3 + 3) + 10 = 22$]

4. (a) Describe the IND-ID-CCA security model of an identity based encryption scheme.

   (b) Describe the BasicIdent scheme.

   (c) Show that BasicIdent is not IND-ID-CCA secure.

[$8 + 10 + 4 = 22$]

INDIAN STATISTICAL INSTITUTE

Semestral Examination: (2017-2018)
M.Tech C.S., 2nd Year

Advanced Digital Signal Processing

Date:20.4.2018 Maximum Marks: 100 Duration: 3 hours

Note: The exam is open book and open notes. The marks add up to 119. The maximum you can score is 100.

Questions:

1. A white noise process of variance 1 is passed through a causal Linear Time Invariant (LTI) system with system function
$$H(e^{j\omega}) = \frac{1}{1 - z^{-1} + 0.6z^{-2}}.$$
to produce the second-order Auto-Regressive (AR(2)) process $x[n]$. Determine the autocorrelation sequence of $x[n]$ using the Yule-Walker equations. [10]

2. Consider a signal
$$x[n] = cos(\pi n/16) + 0.5cos(5\pi n/64) \quad 0 \leq n \leq 128$$
   (a) Determine the location of the single spectral peak obtained using a 64 point DFT with a rectangular window.
   (b) Suggest with justification how it might be possible to resolve both components using a 128 point DFT, and
   (c) state the location of the peaks.

   [5+5+2]

3. The Time-dependent Fourier Transform $X[n, \lambda)$ of a signal
$$x[n] = [cos(\pi n/2)]^2 \quad n \geq 0.$$
is defined as
$$X[n, \lambda) = \sum_{m=-\infty}^{\infty} x[n+m]w[m]e^{-j\lambda m}$$
Let $w[n]$ be a rectangular window *i.e.* $w[n] = 1, \quad 0 \leq n \leq 13$. Defining $X[n, k] = X[n, 2\pi k/7]$ for $0 \leq k \leq 6$.Determine

(a) $X[0,k]$ for $0 \leq k \leq 6$.

(b) $\sum_{k=0}^{6} X[n,k]$ for $0 \leq n < \infty$.

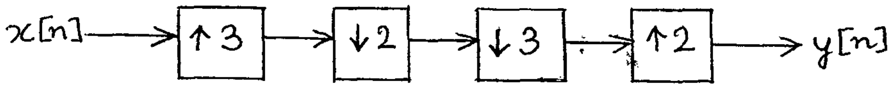
[7+7]

4. Show that the periodogram $I(\omega) = \frac{1}{LU}|V(e^{j\omega}|^2$ of a discrete time random signal $x[n]$, can be also expressed as

$$I(\omega) = \frac{1}{LU} \sum_{m=-(L_1)}^{L-1} c_{vv}[m]e^{-j\omega m}$$

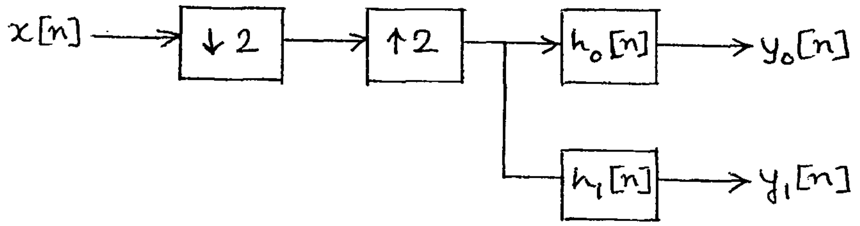
where $v[n] = x[n]w[n]$, $w[n]$ is a rectangular window of length L, U is a normalizing constant and $c_{vv}[m]$ is the aperiodic autocorrelation of $v[n]$. [10]

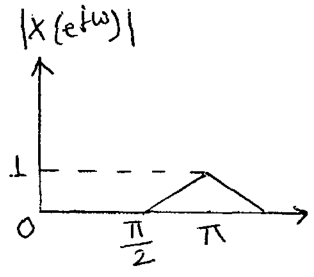
5. Determine $y[n]$ in terms of $x[n]$ for the system given below:

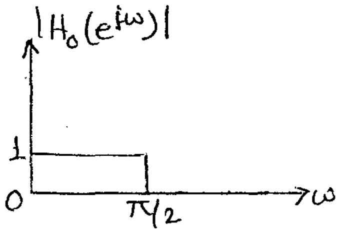


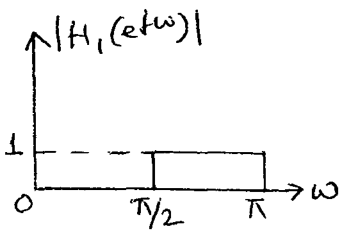
[5]

6. Consider the system shown below. The Discrete Time Fourier Transform (DTFT) of the input and the frequency responses of the two filters $h_0[n]$ and $h_1[n]$ are as sketched. Determine $Y_0(e^{j\omega})$ and $Y_1(e^{j\omega})$.







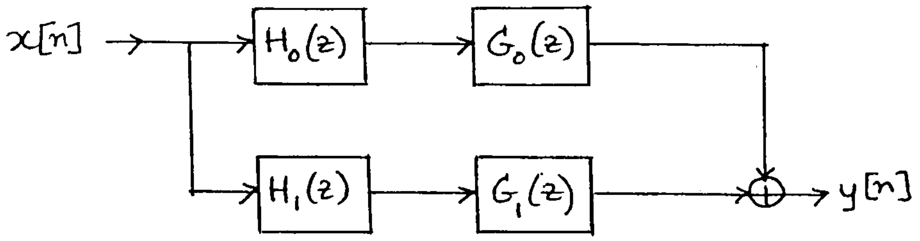


[6+6]

7. For the analysis/synthesis system shown below and

$$H_0(z) = 1 + z^{-1}, \quad H_1(z) = H_0(-z),$$

determine Finite Impulse Response (FIR) synthesis filters such that the system performs perfect reconstruction. [10]



8. For an uniform DFT analysis bank with $M = 4$ and the polyphase components of $H_0(z)$ equalling $E_0(z) = 1 + z^{-1}$, $E_1(z) = 1 + 2z-1$, $E_2(z) = 2 + z^{-2}$ and $E_3(z) = 0.5 + z^{-1}$, obtain expressions for $H_k(z)$, $k = 1, \cdots, 3$ giving explicit values for the coefficients. [10]

9. For the Ramanujan sum

$$c_q[n] = \sum_{\substack{k=1 \\ (k,q)=1}}^{q} e^{j2\pi kn/q}$$

(a) Compute the DFT of $c_q[n]$. Explain how you would choose the length of the DFT.

(b) Show that any two Ramanujan sums $c_{q_1}(n)$ and $c_{q_2}(n)$ are orthogonal, *i.e.*

$$\sum_{n=0}^{m-1} c_{q_1}(n)c_{q_2}(n) = 0, \quad q_1 \neq q_2 \quad m = lcm(q_1, q_2)$$

[(5+1)+8]

10. For a Blind Source Separation (BSS) system with N source signals $s_1, \cdots, s_N$, M microphone observations $x_1, \cdots, x_M$, show that,

$$\mathbf{x}(\tau, f) = \mathbf{h}_{k^*}(f) s_{k^*}(\tau, f) + \mathbf{e}(\tau, f), \quad k^* \in 1, \cdots, N$$

for sparse sources, with k^* representing the most dominant source in time-frequency slot (τ, f). $h_{jk}(f)$ is the frequency response from source k to microphone j, $x_j(\tau, f)$ and $s_j(\tau, f)$ are the Short Time Fourier Transforms of $x_j(t)$ and $s_j(t)$, respectively. Further, $\mathbf{h}_k = [h_{1k}, \cdots, h_{Mk}]^T$, $\mathbf{x} = [x_1, \cdots, x_M]^T$ and $\mathbf{n}$ stands for a noise component. [10]

11. Show that

    (a) The Haar wavelets at different scales are orthogonal, and

    (b) the scaling function is orthogonal to the wavelets.

[7+5]

INDIAN STATISTICAL INSTITUTE

Semestral Examination

M. Tech (CS) - II Year (Semester - II)

Topics in Algorithms and Complexity

Date : April 20, 2018 Maximum Marks : 50 Duration : 3 Hours

Note : You may answer any part of any question, but maximum you can score is 50.

1. Consider the integer line and an infinite random walk on it, starting from 0. Here vertices are integers on the line, and edges connect two consecutive vertices on the line. From a vertex k, one can reach $k-1$ or $k+1$ in one step, each with probability $\frac{1}{2}$. Show that the expected number to visits of vertex 0 in this walk is unbounded.

   [You may use Stirling's approximation $n! = \sqrt{2\pi n}(\frac{n}{e})^n$]

   [10]

2. (a) Define VC dimension $VC(S)$ for a set system $S = (X, R)$, where X is a (finite or infinite) set of elements and R is a (finite or infinite) family of subsets of X.

   (b) Give an example of a set system S with $VC(S) = \infty$.

   (c) Show that, for a set system $S = (X, R)$ with $X =$ a set of points in $\mathbf{R}^3$, and $R =$ all possible half-spaces in $\mathbf{R}^3$, $VC(S) < 5$.

   (d) Let $S = (X, R)$ be a set system with $VC(S) = \delta$. What will be $VC(\overline{S})$ where the set system $\overline{S} = (X, \overline{R})$, and $\overline{R} = \{X \setminus r \ \forall r \in R\}$?

   [4+4+10+6=24]

3. Let $n, d \in \mathbf{Z}^+$ be two positive integers, $d \geq 2$, $\epsilon \in \mathbf{R}^+$. Let $S = (X, R)$ be a range space with VC dimension $VC(S) = d$. If $A \subseteq S$ with cardinality $|A| = n$, then show that there exists an ϵ-net N of A (with respect to the ranges in R) with $|N| \leq \lceil \frac{d \log n}{\epsilon} \rceil$.

   [12]

4. (a) Define fixed parameter tractable (FPT) algorithms for computationally hard optimization problems.

   (b) Given an undirected and unweighted graph $G = (V, E)$ and an integer k (where $|V| = n$ and $k \ll n$), design a linear programming based FPT algorithm for the vertex cover problem on the given graph G that computes a kernel (a subgraph G' of G) of size $O(k)$ where you may apply exhaustive search to compute the optimum solution of the vertex cover of G.

   [4+10=14]

5. In the *cluster editing* problem, we are given a graph $G = (V, E)$ and a positive integer k ($\ll |V|$). The objective is to test whether it is possible to split the graph into disjoint cliques by editing at most k edges. Editing an edge $(u, v), u, v \in V$, means removing $e = (u, v)$ from E if $e \in E$, or adding e to E if $e \notin E$. This decision problem is known to be NP-hard. The objective here is to generate small subgraphs (not necessarily all of them are cliques) of size polynomial in k on which one can execute exhaustive search to solve the *cluster editing* problem.

   Can you suggest an editing scheme that runs in time polynomial in n ($= |V|$), and splits the graph into subgraphs (not necessarily all are cliques) by editing at most k edges such that each subgraph has at most $O(k^2)$ vertices ? Justify your answer.

   [7+8=15]

INDIAN STATISTICAL INSTITUTE
Semester Examination
M. Tech. (CS) II year (2nd Sem): 2017-2018
Logic for Computer Science

Date: 23. 04. 2018 Total Marks : 60 Time : 2.5 Hours

Answer as much as you can. Maximum you can score is 50.

1. (a) What is the meaning of a sequence of elements of a domain satisfying a wff?
   (b) What is the difference between an interpertation and a model?
   (c) What is the difference between truth and logical validity?
   (d) How is the truth of a sentence in first order language objectified and hence separated from personal belief?

   $[4 + 4 + 4 + 4 = 16]$

2. (a) What is the difference between logical axioms and proper axioms?
   (b) What is the meaning of a variable x_i being free in a wff $\mathcal{B}$?
   (c) What is the meaning of a term t being free for a variable x_i in a wff $\mathcal{B}$?
   (d) Is the term $f(x_1, x_3)$ free for x_1 in $\forall x_2 A(x_1, x_2) \implies B(x_1)$ and in $\exists x_3 \forall x_2 A(x_1, x_2) \implies B(x_1)$?

   $[4 + 4 + 4 + 4 = 16]$

3. (a) What is the difference between Prenex Normal Form and Skolem Normal Form?
   (b) Convert the following wff in Prenex Normal Form:
   $$A(x,y) \implies \exists y\,[B(y) \implies \{\exists x B(x) \implies C(y)\}].$$
   (c) Briefly sketch the algorithm for Skolemization with an example.

   $[4 + 4 + 4 = 12]$

4. (a) State and give proof-sketch for Gödel's first incompleteness theorem.
   (b) State and give proof-sketch for Gödel's second incompleteness theorem.
   (c) What is the implication of Gödel's second incompleteness theorem in Artificial Intelligene?

   $[(2 + 4) + (2 + 4) + 4 = 16]$

Indian Statistical Institute

M.Tech (CS) II

Information Security and Assurance

Semester Examination

Maximum Marks: 100

Date: April 27, 2018
Time 3 hours

The question paper contains 6 questions. Total marks is 105. Maximum you can score is 100.

1. Alice has input bits x_1, x_2 and Bob has input bits y_1, y_2. Both Alice and Bob want to compute $z = (x_1 \wedge y_1) \wedge (x_2 \vee y_2)$, securely. Describe a step-by-step procedure for computing z, such that Alice does not know y_1, y_2, Bob does not know x_1, x_2 and none other than Alice and Bob knows z. (15)

2. Three friends Alice, Bob and Charlie want to establish a common key in order to communicate securely. Can you design a one-round protocol? Discuss the security of your algorithm. (7 + 8 = 15)

3. N communicating nodes $\mathcal{N} = \{n_1, n_2, \ldots, n_N\}$ collect data and send to an aggregator node n_a. The aggregator node has to verify the integrity of data collected from $\mathcal{N}$. How can you do so using BLS signatures? What is the complexity of the verification algorithm? Can you design an efficient algorithm to reduce the verification time? What is the time complexity of the new verification algorithm? (3 + 4 + 4 + 4 = 15)

4. (a) What are the challenges in storing data in untrusted servers, for example clouds?

   (b) I have stored a large file F in an untrusted server. I do not have a local copy on my disk. How can I verify the integrity of F without downloading the whole file?

   (c) What is the communication and computation complexitity of the procedure. (5 + 10 + 5 = 20)

5. How will you search for keywords in encrypted documents? Does inverted index improve the efficiency of the search? If so, justify. What are the possible information leakages in both the cases? (10 + 5 + 10 = 25)

6. Alice wants to delegate the task of adding two numbers to an untrusted party Bob. Write an algorithm to do so, and discuss the security of the algorithm. (10 + 5 = 15)